D-Link®

Version 1.00| 09/18/2014

User Manual

D-Link Central WifiManager

Table Of Contents

Product Overview **3**
System Requirements 3
Software Installation **4**
Central WifiManager Server Installation 5
Access Point Module Installation 11
Central WifiManager Server Application 13
Access Point Installation Tool 15
Central WifiManager Configuration **19**
Home 20
Dashboard 20
Site 21
Device View 21
Topology View 22
Configuration 24
Site 24
Create Site 25
Network 27
Create Network 28
SSID 30
Create SSID 31
VLAN 43
Bandwidth Optimization 47
Captive Portal 48
RF Optimization 49
Device Settings 50
Upload Configuration 52
Firmware Upgrade 53
Undefined AP 55
System 56
Settings 56
General 56
Module 57
Database 58
Advanced 60
SMTP 61
User Manager 62
Create User Account 63
Monitor 64
Report 64
Association 64
By Access Point 64
By Wireless Station 65
By Station Number 66
Security 67
Chart 67
List 68
Channel 69
Rogue AP 70
New AP 70
Rogue AP 74
Valid AP 75
Neighbor AP 76
SysLog 77
Monitor 78
Monitor Manager 78
Create Profile 79
Monitor List 80
Event 82
Type 82
Standard 82
Event 83
Notice 84
Private 85
Event 86
Notice 87
Watch 88
Watch Manager 88
Create Watch 89
Watch List 92
About 94
Appendix A - Front Desk Staff & User Access **95**
Appendix B - Standard & Private Trap List **105**

Product Overview

The D-Link Central WifiManager is a versatile, convenient software solution for administrators to manage wireless devices throughout the network from a central point.

System Requirements

For the best results, the following minimum requirements are recommended on the computer used to run the Central WifiManager Server application:

- Hardware:
  - CPU: Intel Core i5 3.2GHz.
  - RAM: 4Gb DDR3.
  - HDD Space: 2 Terrabytes.
  - Display Card: Windows Graphics Card.
  - Installed Gigabit Network Adapter.
- Operating System:
  - Microsoft® Windows XP (SP2).
  - Microsoft® Windows Vista.
  - Microsoft® Windows 7 (Ultimate/Enterprise) (x86/x64).
  - Microsoft® Windows Server 2008 (R2 with SP2) (x64).
  - Microsoft® Windows Server 2012 (R2) (x64).
  - Mac OS X 10.5.6.

Software Installation

In the following section, we'll discuss the software that needs to be installed and used to successfully run the Central WifiManager application.

The following software applications must be installed in order:

- The **Central WifiManager Server** application. This is the main application that will be responsible for day-to-day wireless network management and maintenance. For more information, refer to "**Central WifiManager Server Installation**" on page 5 and "**Central WifiManager Configuration**" on page 19.
- The **Access Point Module** software for all access points that will be used in the Central WifiManager Server application. Every access point has its own access point module software that can be installed on the computer that hosts the Central WifiManager Server application. These modules allow seamless communication between the server and the access points using the Simple Network Management Protocol (SNMP). For more information, refer to "**Access Point Module Installation**" on page 11.
- The **Access Point Installation Tool**. This utility can be used to find new access points on the network, change the IP address of each access point, and upload the network data file for each access point. For more information, refer to "**Access Point Installation Tool**" on page 15.

Included at the end of this document, we have the following appendices with additional information that can be helpful to the reader:

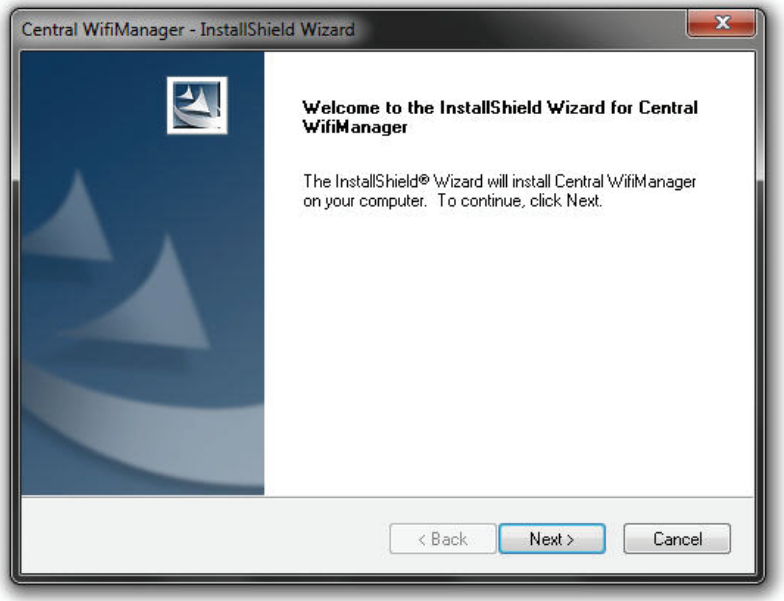
- "**Appendix A - Front Desk Staff & User Access**" on page 95.
- "**Appendix B - Standard & Private Trap List**" on page 105.

Software Installation

Central WifiManager Server Installation

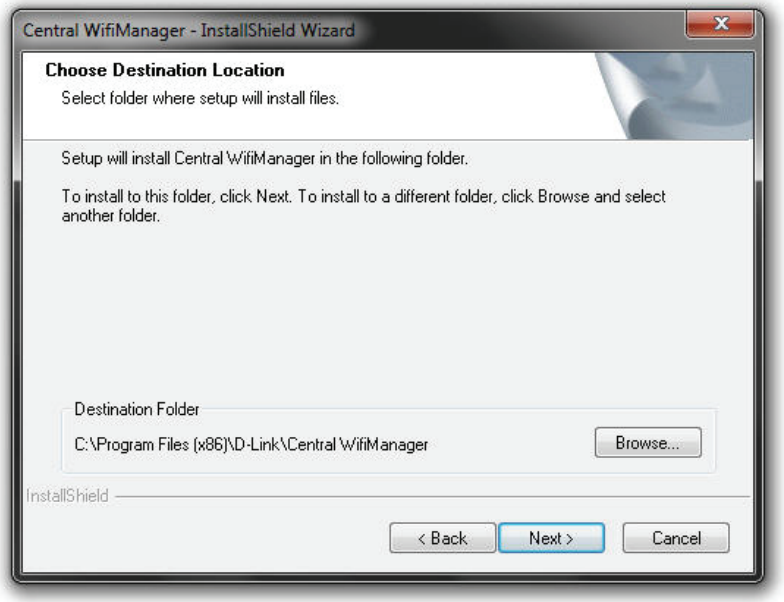
In this section, we'll discuss the installation procedure for the D-Link Central WifiManager software. After running the installation file, a welcome window will be displayed.

Click the **Next >** button to continue to the next step.
Click the **Cancel** button to stop and exit the installation.


Central WifiManager - InstallShield Wizard
Welcome to the InstallShield Wizard for Central WifiManager
The InstallShield® Wizard will install Central WifiManager on your computer. To continue, click Next.
< Back
Next >
Cancel

In this window, the destination location is displayed, where the software will be installed. If this application needs to be installed at a different location or on a different drive, click the **Browse** button and navigate to the new destination location.

Click the **< Back** button to return to the previous step.
Click the **Next >** button to continue to the next step.
Click the **Cancel** button to stop and exit the installation.

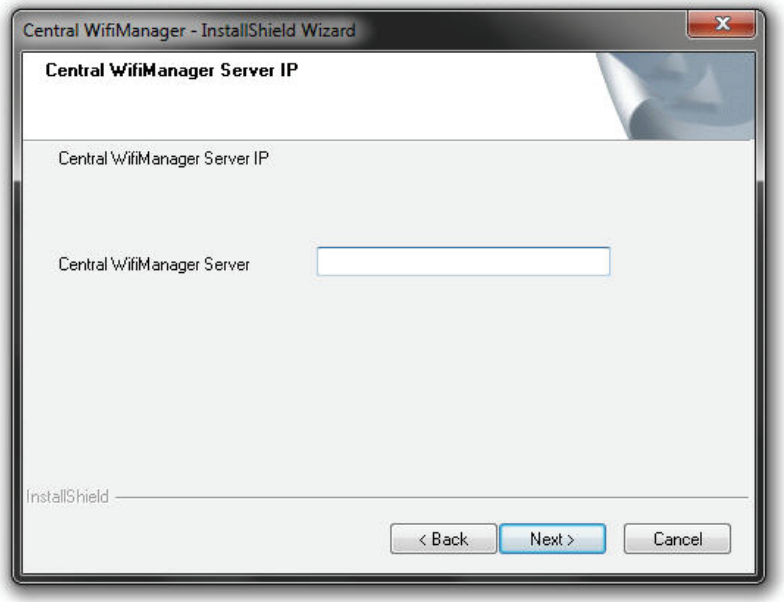

Central WifiManager - InstallShield Wizard
Choose Destination Location
Select folder where setup will install files.
Setup will install Central WifiManager in the following folder.
To install to this folder, click Next. To install to a different folder, click Browse and select another folder.
Destination Folder
C:\Program Files (x86)\D-Link\Central WifiManager
Browse...
InstallShield
< Back
Next >
Cancel

Software Installation

Central WifiManager Server Installation

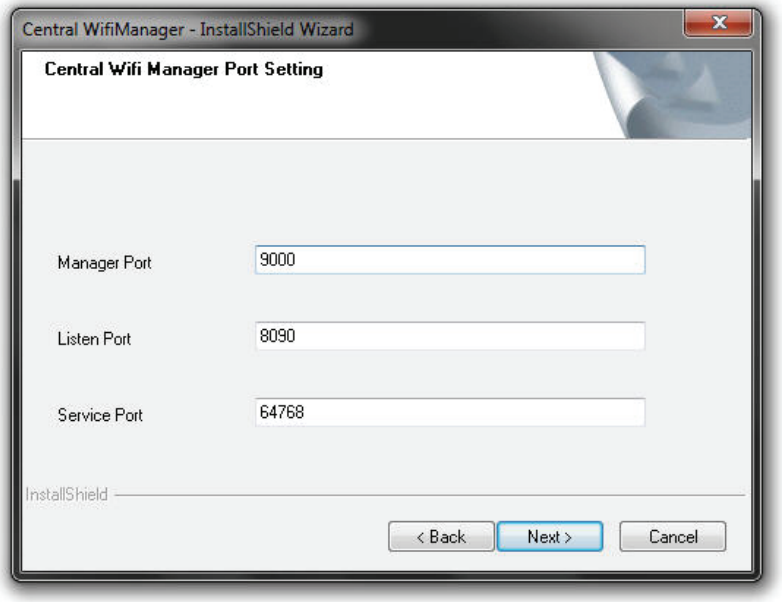
In this window, we need to enter the IP address for the Central WifiManager in the **Central WifiManager Server** space provided. This is normally the IP address of the PC being used for the installation.

Click the **< Back** button to return to the previous step.
Click the **Next >** button to continue to the next step.
Click the **Cancel** button to stop and exit the installation.



In this window, we can view or modify the **Manager**, **Listen** and **Service Port** numbers.

Click the **< Back** button to return to the previous step.
Click the **Next >** button to continue to the next step.
Click the **Cancel** button to stop and exit the installation.

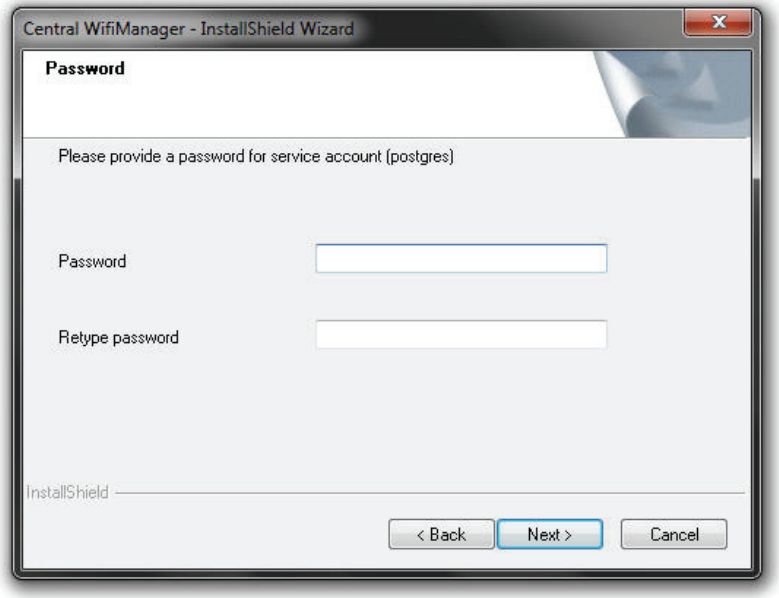


Software Installation

Central WifiManager Server Installation

In this window, we must enter the PostgreSQL password that will be associated with this application in the spaces provided. Enter the same password in the **Password** and **Retype password** spaces provided.

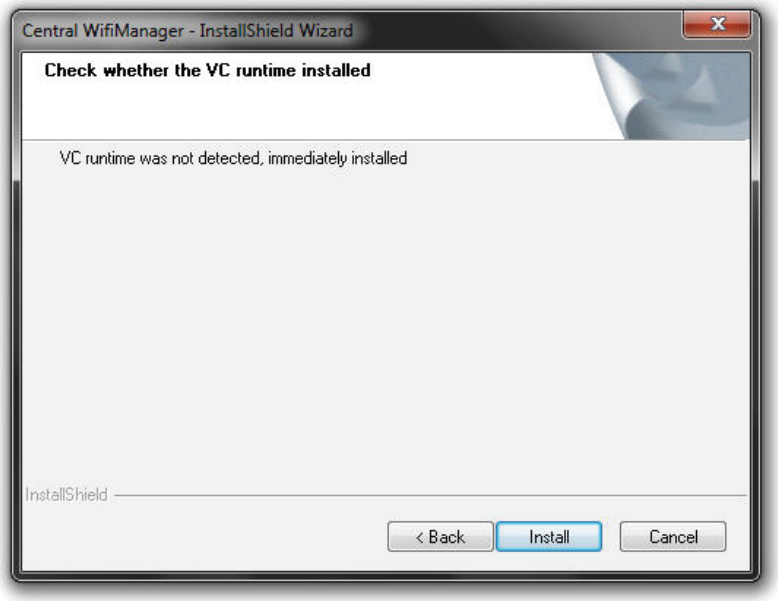
Click the **< Back** button to return to the previous step.
Click the **Next >** button to continue to the next step.
Click the **Cancel** button to stop and exit the installation.



The installation of this application requires Microsoft Visual C++ 2008 Redistributable to be installed on this computer. In this step, the installation wizard will check if the redistributable is installed on this computer. If found, this step will be skipped.

If not found, the option will be given to install the required redistributable..

Click the **< Back** button to return to the previous step.
Click the **Install** button to continue to the next step.
Click the **Cancel** button to stop and exit the installation.

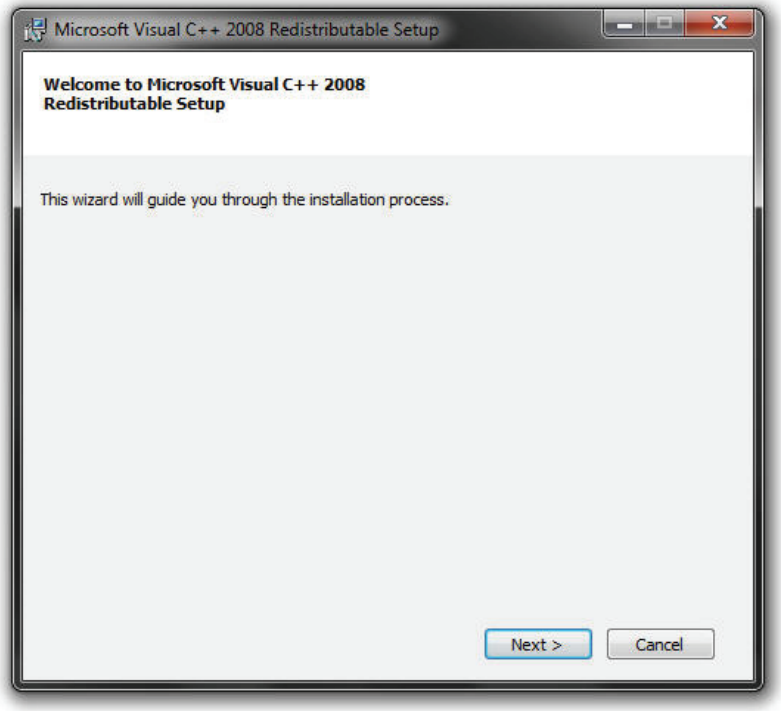


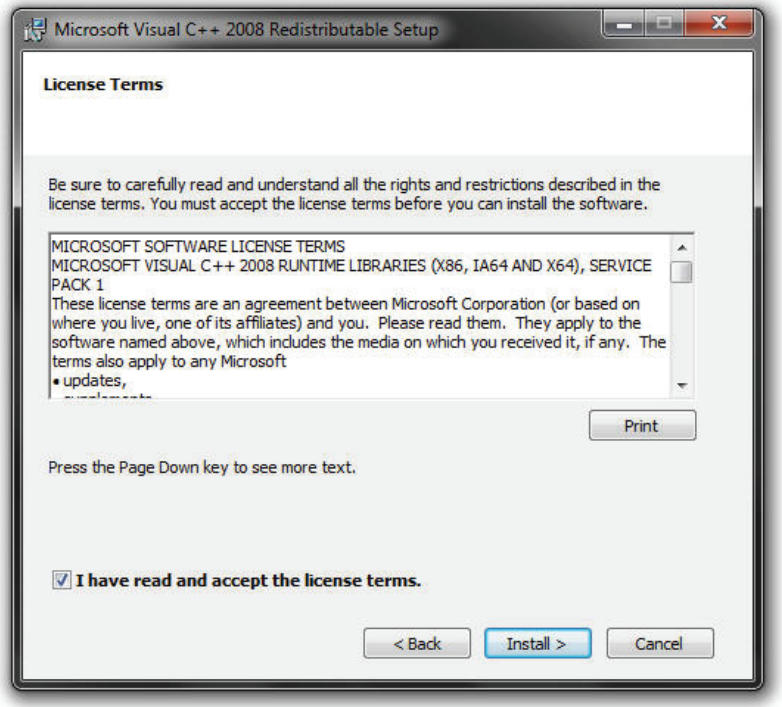
Software Installation

Central WifiManager Server Installation

In this window, a welcome message will be displayed to inform the user that the Microsoft Visual C++ 2008 Redistributable will be installed.

Click the **Next >** button to continue to the next step.
Click the **Cancel** button to stop and exit the installation.


Microsoft Visual C++ 2008 Redistributable Setup
Welcome to Microsoft Visual C++ 2008 Redistributable Setup
This wizard will guide you through the installation process.
Next >
Cancel


Microsoft Visual C++ 2008 Redistributable Setup
License Terms
Be sure to carefully read and understand all the rights and restrictions described in the license terms. You must accept the license terms before you can install the software.
MICROSOFT SOFTWARE LICENSE TERMS
MICROSOFT VISUAL C++ 2008 RUNTIME LIBRARIES (X86, IA64 AND X64), SERVICE PACK 1
These license terms are an agreement between Microsoft Corporation (or based on where you live, one of its affiliates) and you. Please read them. They apply to the software named above, which includes the media on which you received it, if any. The terms also apply to any Microsoft
• updates,
Print
Press the Page Down key to see more text.
I have read and accept the license terms.
< Back
Install >
Cancel

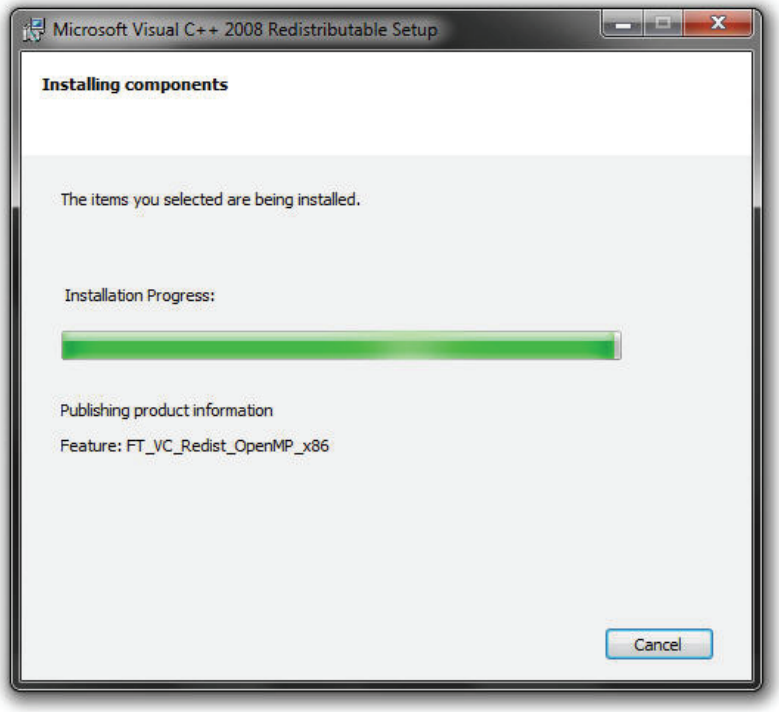
In this window, the license terms of the redistributable package will be displayed. Read through the terms, print if needed, and select the **I have read and accept the license terms** check box to continue with the installation.

Click the **< Back** button to return to the previous step.
Click the **Install >** button to continue to the next step.
Click the **Cancel** button to stop and exit the installation.

Software Installation Central WifiManager Server Installation

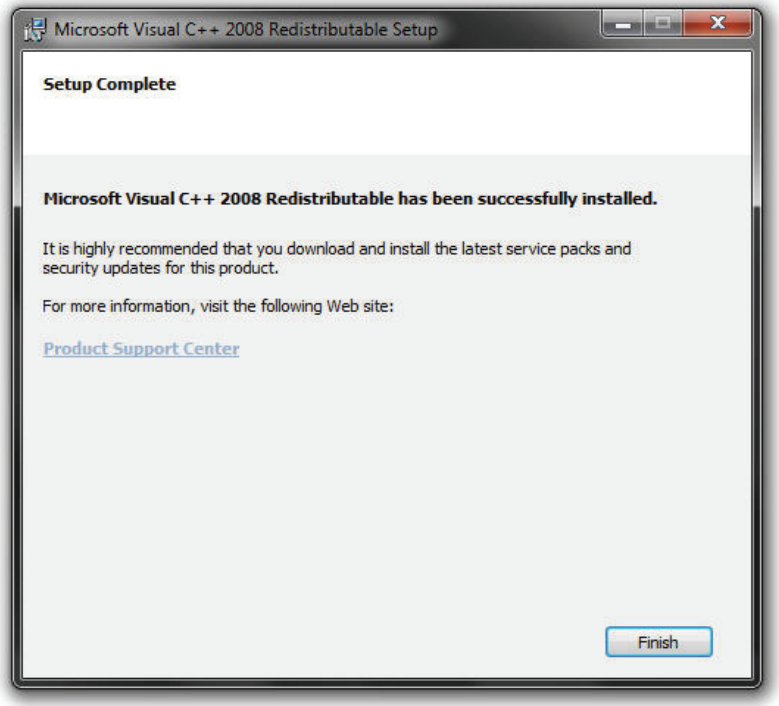
The redistributable package will now be installed.

Click the **Cancel** button to stop and exit the installation.



After the redistributable package was installed, this window will appear. In this window the user is reminded that there might be updates available for this redistributable package and that it is highly recommended to update it.

Click the link to find out if there are updates available for the redistributable package. Click the **Finish** button to complete the redistributable package installation and continue to the next step of the Central WifiManager software installation.

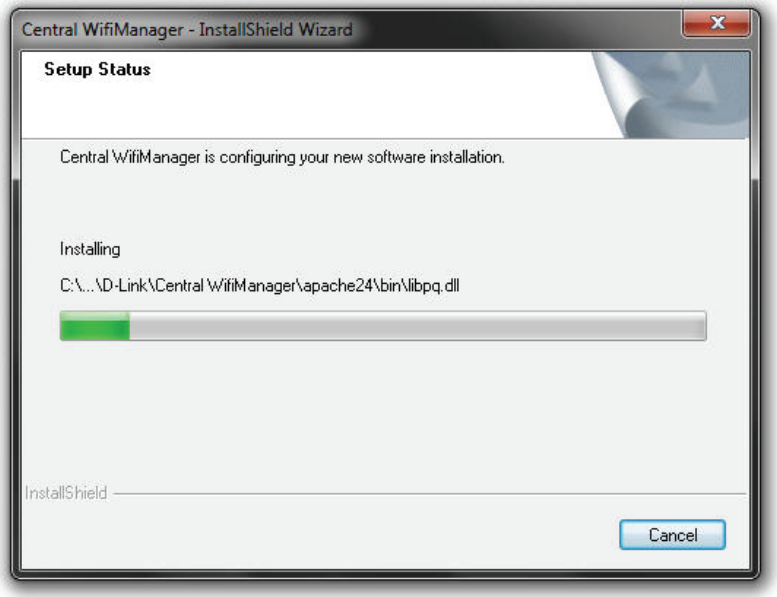

Microsoft Visual C++ 2008 Redistributable Setup
Setup Complete
Microsoft Visual C++ 2008 Redistributable has been successfully installed.
It is highly recommended that you download and install the latest service packs and security updates for this product.
For more information, visit the following Web site:
Product Support Center
Finish

Software Installation

Central WifiManager Server Installation

After the Microsoft Visual C++ 2008 Redistributable was installed the Central WifiManager software installation will continue.

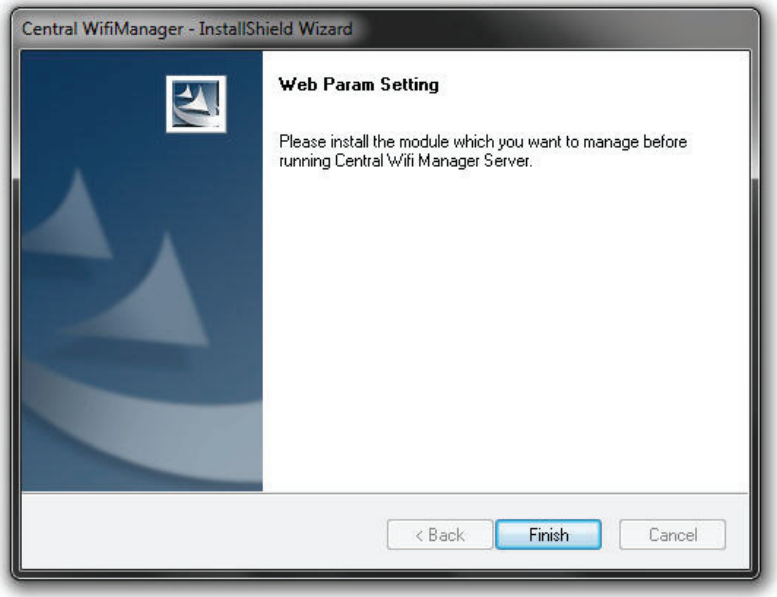
Click the **Cancel** button to stop and exit the installation.



The Apache HTTP Server application might be blocked by the computer's firewall. If Windows' default firewall is used, a security alert message will be displayed. Click the **Allow Access** button to allow this application to communicate with the network.

In this window, the user is reminded that apart from the Central WifiManager installation, each access point that will be used in this application requires a separate module to be installed. This will be discussed in the next section.

Click the **Finish** button to complete and exit the installation wizard.


Central WifiManager - InstallShield Wizard
Web Param Setting
Please install the module which you want to manage before running Central Wifi Manager Server.
< Back
Finish
Cancel

Software Installation

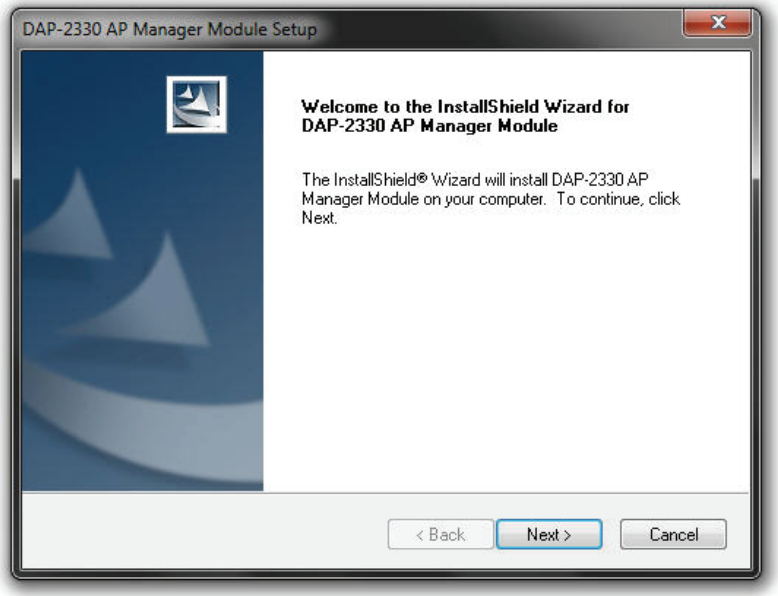
Access Point Module Installation

For each access point that will be used in the D-Link Central WifiManager, we need to install an additional manager module. In this section we'll discuss the installation of the DAP-2330AP access point's manager module that will be used in the D-Link Central WifiManager.

NOTE: If the Central WifiManager Server is already running, it must be stopped and closed before that Access Point manager module can be installed.

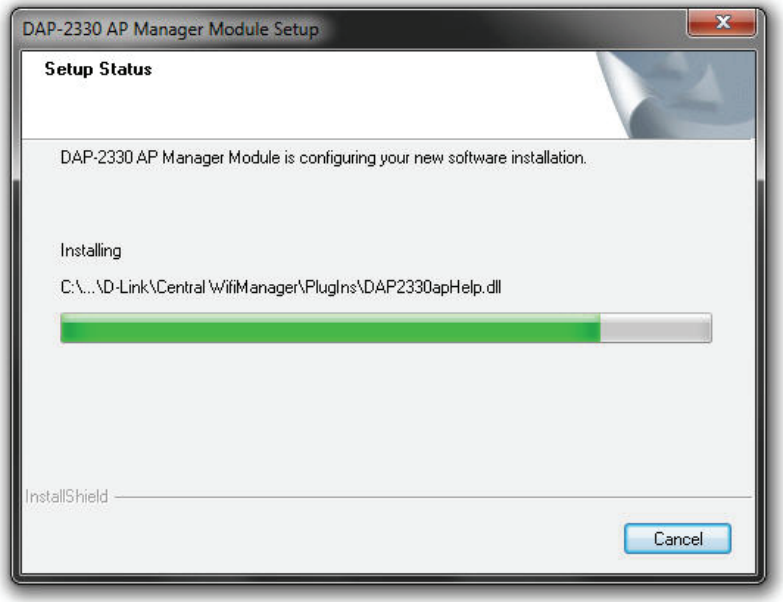
After running the access point's manager module, a welcome message will be displayed to inform the user that the manager module will now be installed on the computer.

Click the **Next >** button to continue to the next step.
Click the **Cancel** button to stop and exit the installation.


DAP-2330 AP Manager Module Setup
Welcome to the InstallShield Wizard for DAP-2330 AP Manager Module
The InstallShield® Wizard will install DAP-2330 AP Manager Module on your computer. To continue, click Next.
< Back
Next >
Cancel

After clicking next in the previous step the access point's manager module will be installed.

Click the **Cancel** button to stop and exit the installation.

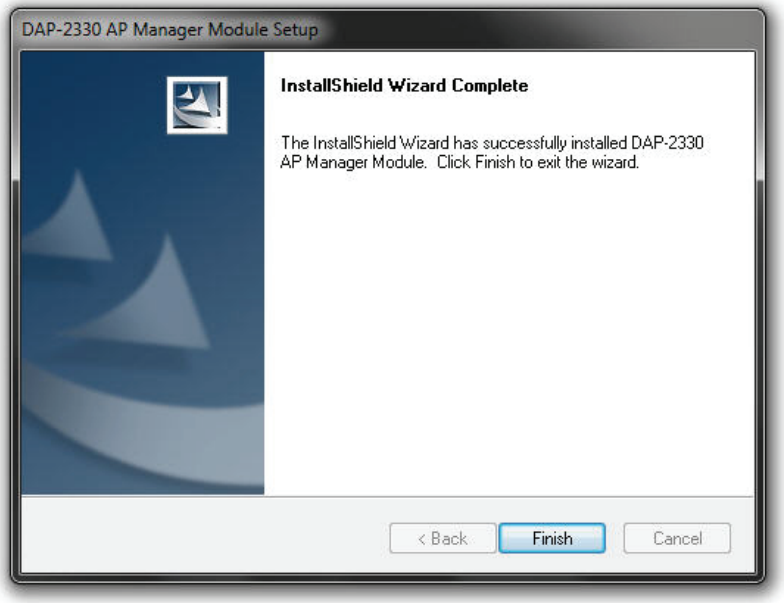


Software Installation

Access Point Module Installation

After the access point's manager module was installed successfully, this window will appear.

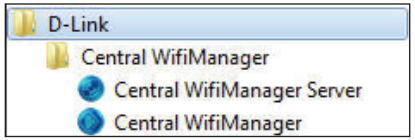
Click the **Finish** button to complete and exit the installation wizard.


DAP-2330 AP Manager Module Setup
InstallShield Wizard Complete
The InstallShield Wizard has successfully installed DAP-2330 AP Manager Module. Click Finish to exit the wizard.
< Back
Finish
Cancel

Software Installation

Central WifiManager Server Application

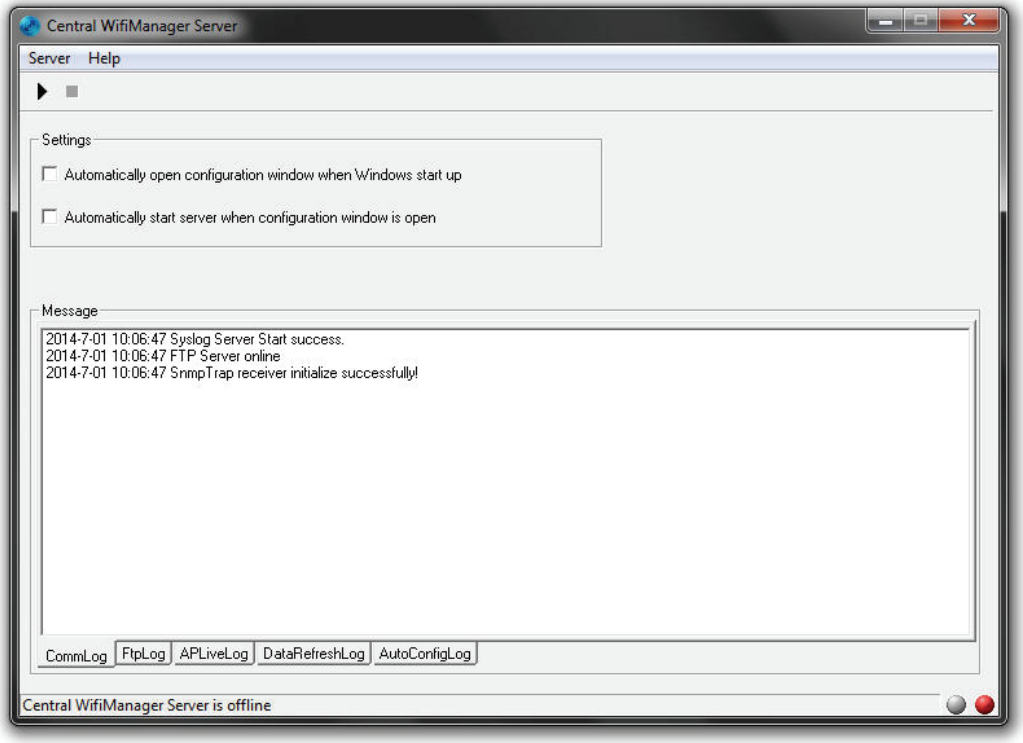
In this section, we'll discuss the Central WifiManager Server application.
After the installation was completed the following applications will be available.



Click the **Central WifiManager Server** option to open the server application.

After running the Central WifiManager Server application, the window (on the right) will appear. This is the management console window for the server application.

In the **Menu** bar, there are two option available, **Server** and **Help**. Under the **Server** menu we can **Start**, **Stop** or **Exit** the application. Alternatively, right under the **Server** menu option, there are also start and stop icons that do exactly the same thing. Under the **Help** menu option, there is an **About** option that will, after being clicked, display the name, version and copyright details of this application.


Central WifiManager Server
Server Help
Settings
Automatically open configuration window when Windows start up
Automatically start server when configuration window is open
Message
2014-7-01 10:06:47 Syslog Server Start success.
2014-7-01 10:06:47 FTP Server online
2014-7-01 10:06:47 SnmpTrap receiver initialize successfully!
CommLog FtpLog APLiveLog DataRefreshLog AutoConfigLog
Central WifiManager Server is offline

Software Installation

Central WifiManager Server Application

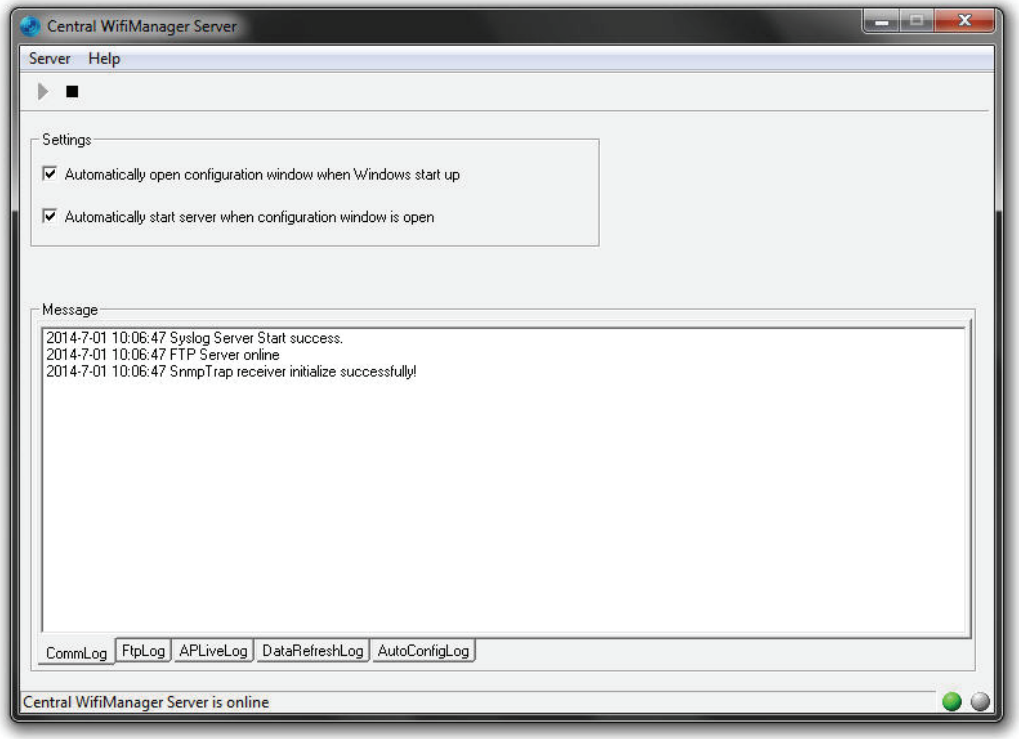
In the **Settings** section, we can select to **Automatically open configuration window when Windows start up** and **Automatically start server when configuration window is open**. Select these options if needed.

After this, there server can be started by click either the start icon or being selecting **Start** in the **Server** menu option.

NOTE: When clicking the close icon, on the far upper right corner, this application will close and exit. The server will not be running in the background. Click the minimize icon to close this window and allow the server application to run in the background.

When the server is up and running, the left circle icon, at the far bottom right corner, will display green. When the server is not running the right circle icon, at the far bottom right corner, will display red.

To view log entries about the System, FTP Connectivity, Live Access Points, Data Transmissions and Automatic Configurations, tabs at the bottom of the **Message** section can be selected.

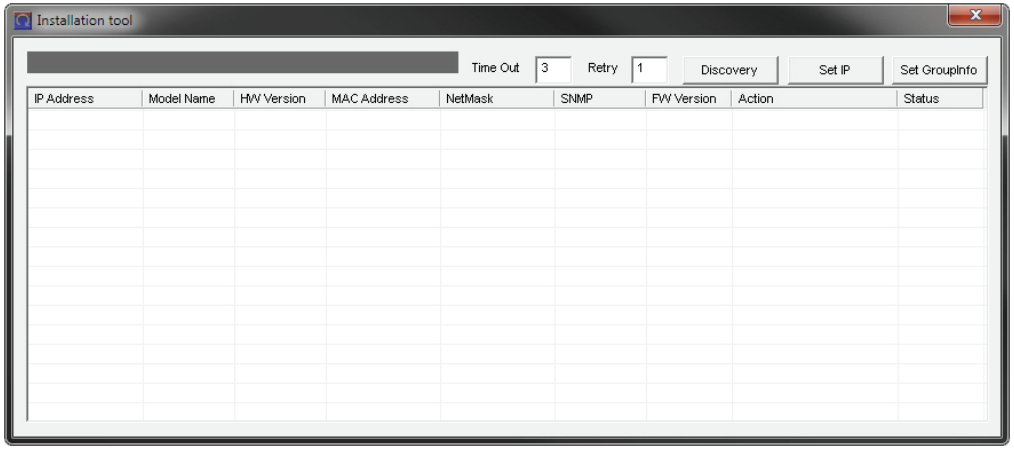


Software Installation

Access Point Installation Tool

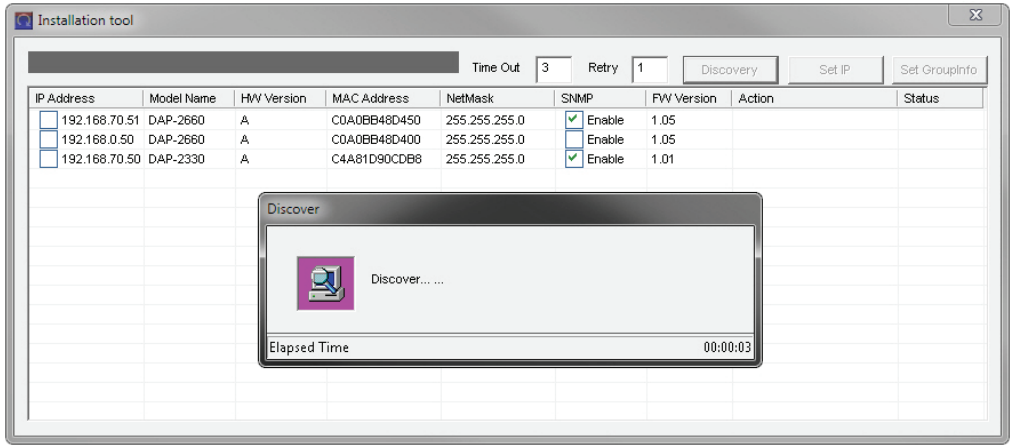
The Access Point Installation Tool is an additional utility that compliments the D-Link Central WifiManager. This utility can be used to scan for new D-Link access points in the network, regardless of what IP range they are configured in, and then pre-configure them to be used in the Central WifiManager.

After opening the Access Point Installation Tool, the following window will be available.



Click the **Discovery** button, to scan for D-Link access points that are connected to the network with an Ethernet cable.

After clicking the **Discovery** button, this utility will scan the network for D-Link access points that are connected to the network with an Ethernet cable. This utility will find D-Link access points regardless of what IP address they're configured in.

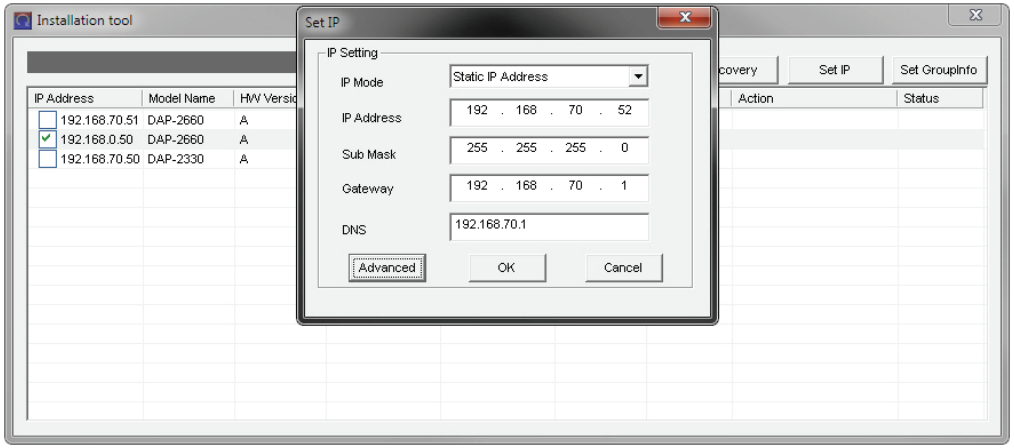


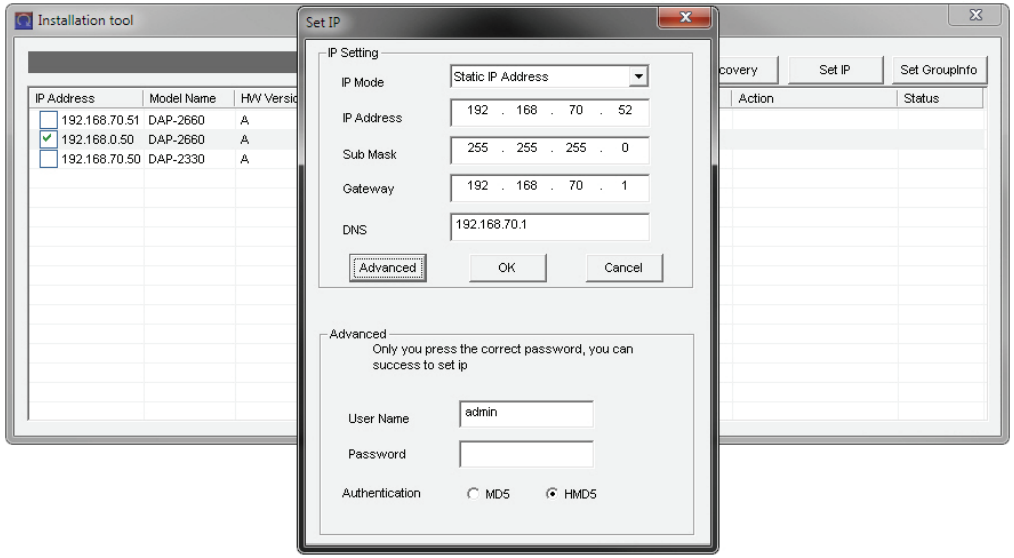
Software Installation Access Point Installation Tool

To change the IP address of an access point discovered, select the check box next to it and click the **Set IP** button.

After clicking the Set IP button, the following parameters can be configured:

Parameter	Description
IP Mode	Select the IP mode for the access point here. Options to choose from are **Static IP Address**, to manually configure the IP settings, and **Dynamic IP Address**, to allow a DHCP server to automatically assign the IP settings to the access point.
IP Address	Enter the new IP address for the access point here.
Sub Mask	Enter the new subnet mask for the access point here.
Gateway	Enter the gateway's IP address for the access point here.
DNS	Enter the DNS address for the access point here.
User Name	After clicking the **Advanced** button, we can enter the login username of the access point here.
Password	After clicking the **Advanced** button, we can enter the login password of the access point here.
Authentication	After clicking the Advanced button, we can select the login authentication encryption method used. Options to choose from are **MD5** and **HMD5**.



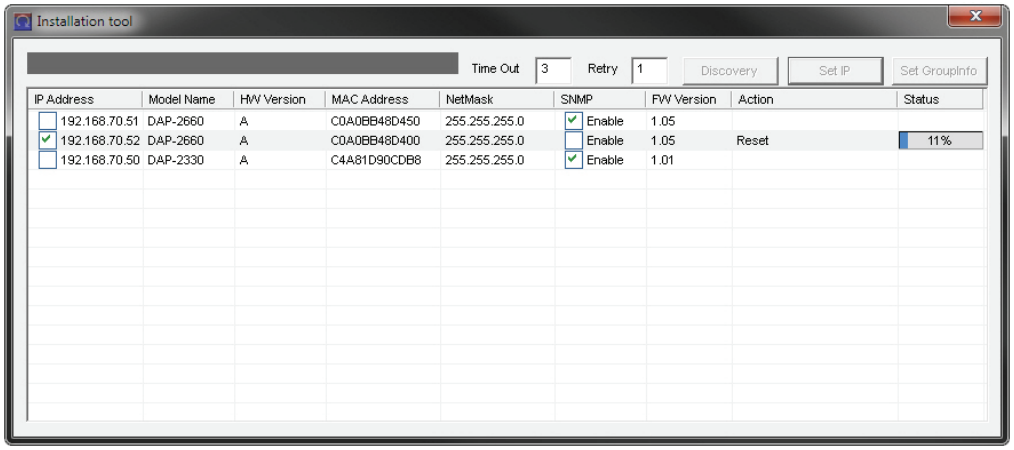


Click the **OK** button to accept the changes made.
Click the **Cancel** button to discard the changes made.

Software Installation
Access Point Installation Tool

After clicking the **OK** button to set the IP address, the access point will be configured and some time will be given for the access point to restart after the new IP address was applied.

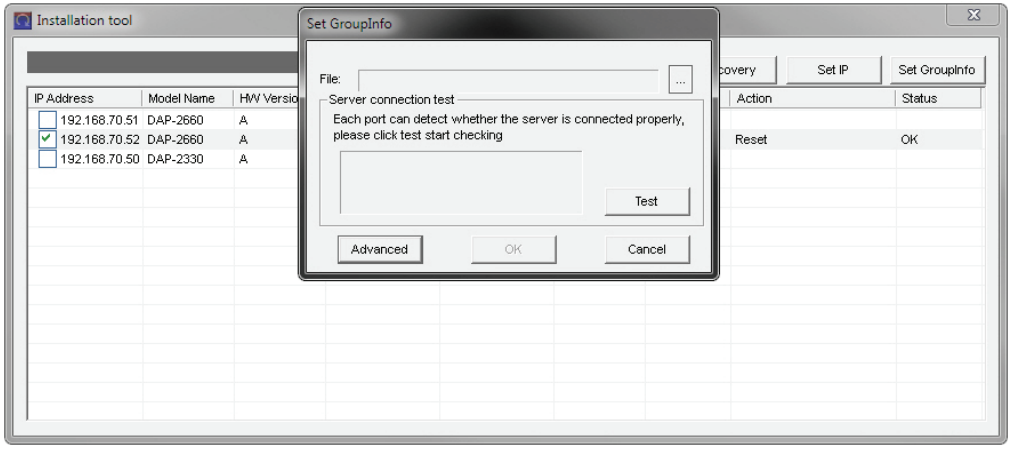
The **Status** parameter will display the progress of the IP address configuration and access point reboot.



This utility also allows us to upload the network data file directly to the access point to configure the group information that this access point will use to identify in which network it belongs.

Click the **Set GroupInfo** button to upload the network data file. After click the Set **GroupInfo** button, we can click on the "**...**" button to navigate to the saved network data file on the computer and then upload it.

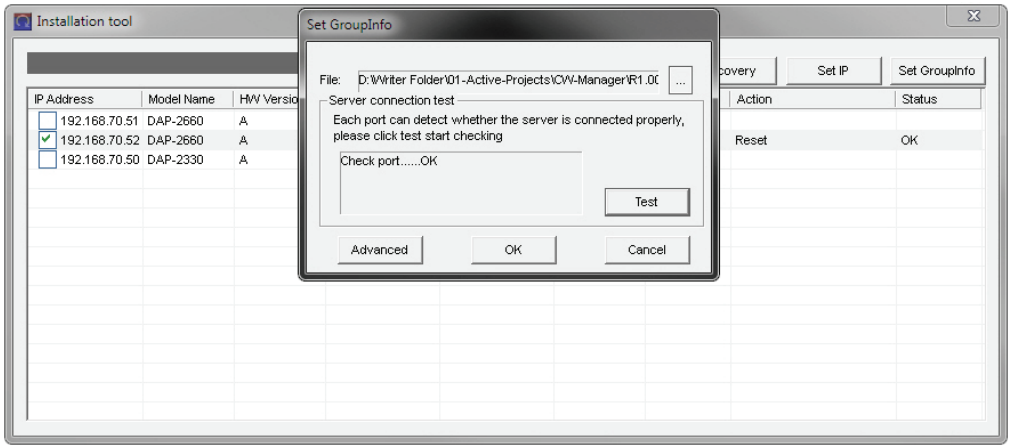
Click the **Test** button to test if the data file is in fact a valid network data file.
Click the **Advanced** button to use advanced login options for the access point as discussed earlier.



Software Installation Access Point Installation Tool

After clicking the **Test** button to successfully test if the network data file is valid, the following message will be displayed.

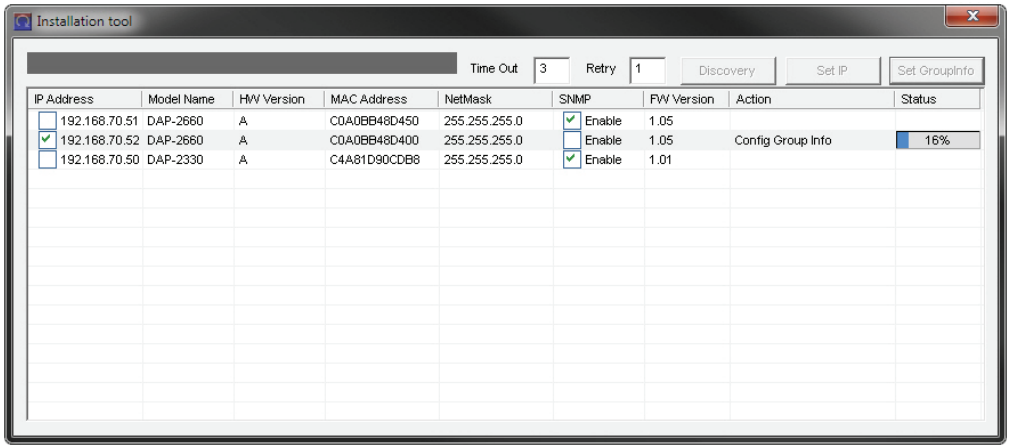
Click the **OK** button to initiate the upload
Click the **Cancel** button to cancel the upload.



After clicking the OK button, the network data file will be uploaded, the access point will be configured based on the settings within the data file, and will then reboot.

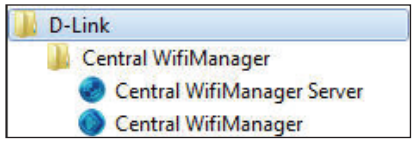
The **Status** parameter will display the progress of the configuration.

For more information about configuring networks and generating network data files used in this upload, refer to “**Network**” on page 27.



Central WifiManager Configuration

In this section, we'll discuss the Central WifiManager client application.
After the installation was completed the following applications will be available.



Click the **Central WifiManager** option to open the client application.

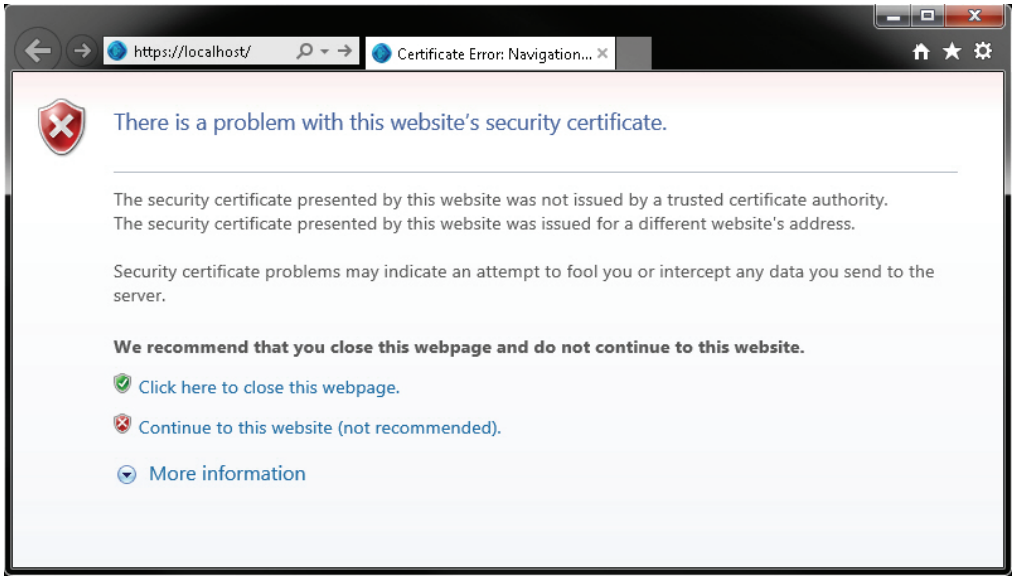
The Central WifiManager uses a secure HTTPS connection to the Central WifiManager Server. By default, this application will open the default Web browser and connect the to **localhost**, which is the local means of connecting to the same PC's own IP address. <$$$Certificate information needed$$$>

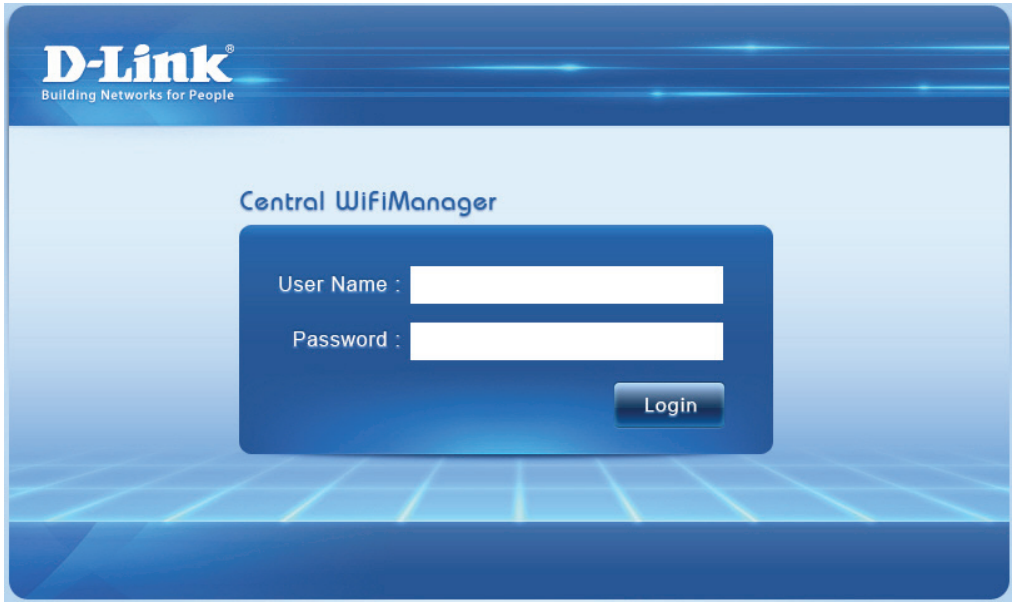
Alternatively, from a remote computer, we can connect to the Central WifiManager Server by entering the IP address of the computer that has the server application installed into the web browser, thus it is not needed to install the software on the remote computer.

NOTE: Connection to the Central WifiManager Server uses a secure HTTPS connection.

After the Web browser was open and connection to the server was made successfully, a login window will appear. Enter the login user name and password in this spaces provided and click **Login** to enter the Central WifiManager Configuration.

NOTE: By default, the user name and password is **admin**.


https://localhost/
Certificate Error: Navigation...
There is a problem with this website's security certificate.
The security certificate presented by this website was not issued by a trusted certificate authority.
The security certificate presented by this website was issued for a different website's address.
Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.
We recommend that you close this webpage and do not continue to this website.
Click here to close this webpage.
Continue to this website (not recommended).
More information



CWM Configuration Home Dashboard

After successfully logging into the server, the **Dashboard** page will be available. On this page, summarized information of the connected access points and wireless clients will be displayed.

After configuring sites, a list of sites will be available for selection in the site drop-down menu.

Underneath the site drop-down menu, the following four blocks with pie charts can be seen.

Block	Description
Station	In this block the number of wireless clients, connected to the access points in this network, will be displayed per wireless frequency supported. The pie chart illustrate this information visually.
Band	In this block the number of wireless frequency bands, hosted by the access points in this network, will be displayed per frequency band supported. The pie chart illustrates this information visually.
Model	In this block the number of access points in this network will be displayed per product code. The pie chart illustrates this information visually.
Access Point	In this block the number of online and offline access points will be displayed per status. The pie chart illustrates this information visually.

In the **Station Detail** table, a list of connected wireless clients will be displayed with the basic information about them.

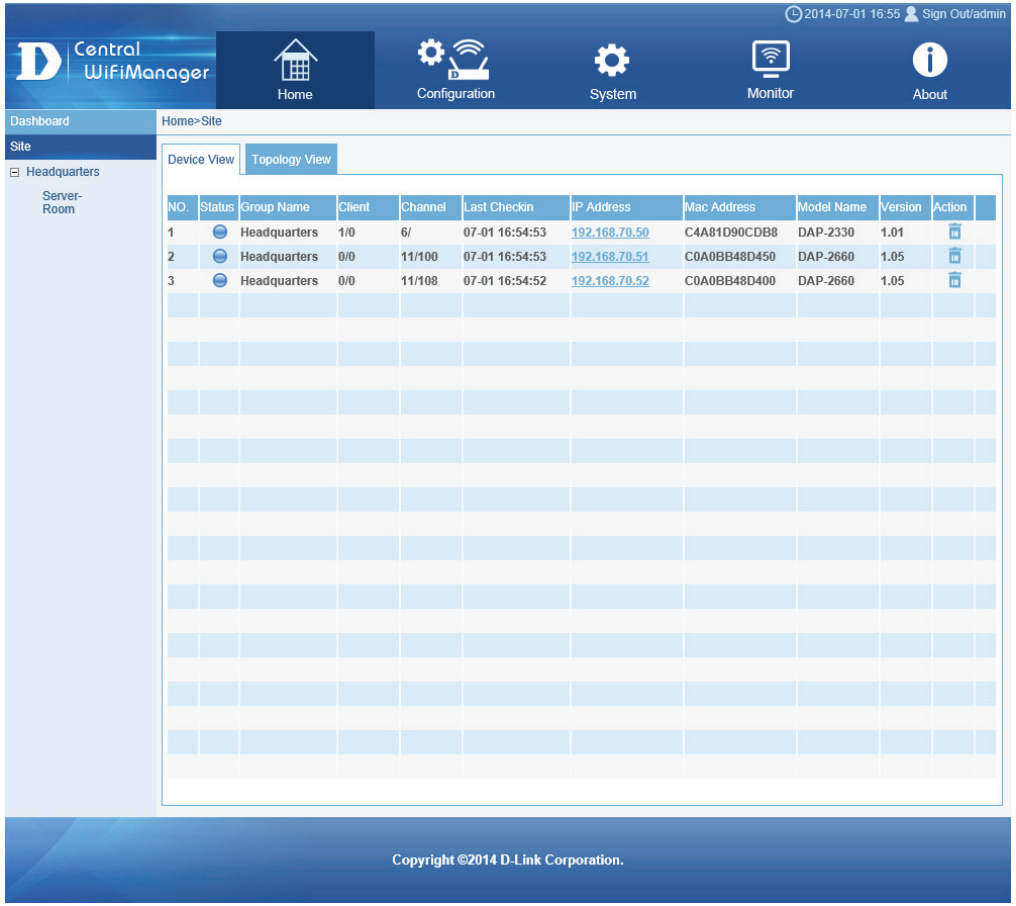
CWM Configuration | Home | Site | Device View

On this page, a list of configured sites will be displayed. For more information on how to create or configure sites, refer to "**Create Site**" on page 25. For this example, we created a site called **Headquarters** and within the site we created a network called **Server-Room**.

For more information on how to create or configure networks, refer to "**Create Network**" on page 28.

In the **Device View** tab, a list of access points will be displayed that was associated with the **Headquarters** site. More information about the access points will be displayed in the table columns. To view more detailed information about a specific access point, click on the IP address of that access point.

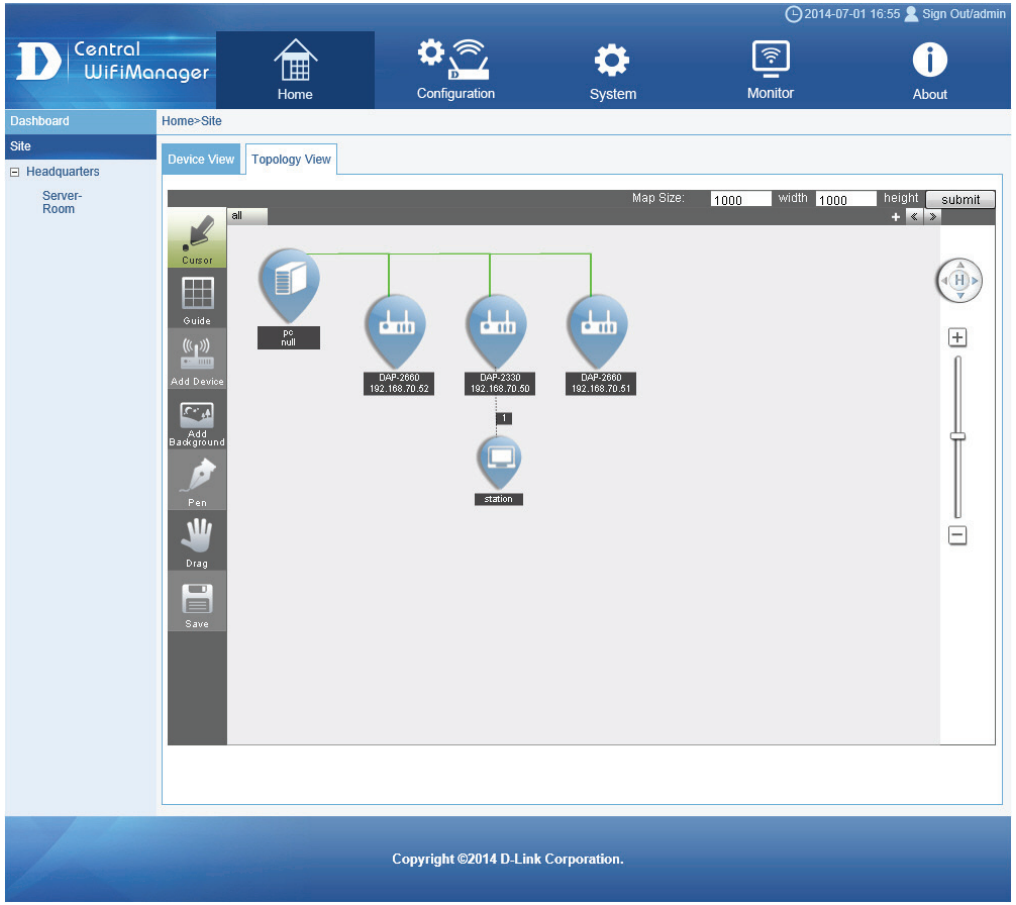
Click the icon to remove an access point from this network.



CWM Configuration | Home | Site | Topology View

On this page, all the devices connected to the specified site will be displayed visually. The following items can be found on this page.

Item	Description
Add Topology	On the top, right of the viewing area, there is a **+** icon. Click this icon to add a custom topology.
Edit Topology	On the top, right of the viewing area, there is an **i** icon. Click this icon to modify the newly added topology's name.
Delete Topology	On the right of the topology tabs, there is an **x** icon. Click this icon to remove the custom topologies created. The **all** topology, which is automatically generated, cannot be deleted.
Map Size	The map size of the topology view can be modified. Enter the **width** and **height** of this view in the text boxes and click **Submit** to accept the changes made. These values must be between 800 and 8000.
Cursor	Select this option to select an item individually.
Guide	Select this option to make the guides visible in the topology.
Add Device	Select this option to add access points, that have been associated with this site, into the topology.
Add Background	Select this option to add a custom background image to the topology. Image formats supported are JPG, JPEG, GIF and PNG.
Pen	Select this option to manually draw a connection line from one device to another. After drawing the connection line, it can be specified as either wired or wireless and the color and line thickness can be customized.



CWM Configuration | Home | Site | Topology View

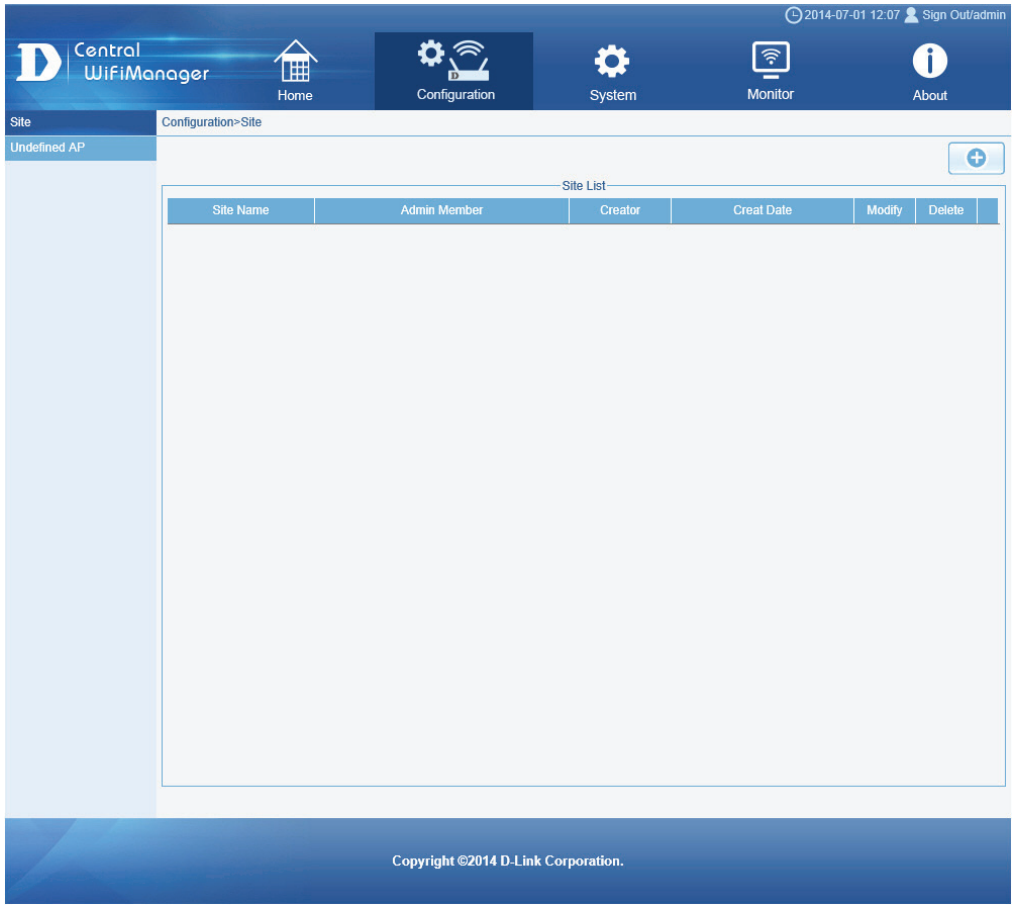
Parameter	Description
Drag	Select this option to enable the function to simply select and move the objects and the background of the topology into place.
Save	Select this option to save the topology.
PC (Null)	This icons illustrates the management PC, where the Central WifiManager Server application is installed.
Access Points	These icons illustrate the access points located at the site and there connection relation with each other. Double click on any access point icon to view more detailed information about the selected access point.

CWM Configuration Configuration Site

On this page we can view, create and configure logical sites and networks that are related to the physical locations of the wireless devices in the network. Wireless devices at these sites can unanimously and effortless be managed and maintained through the use of this application.

Sites and networks that have already been configured will be displayed under the **Site** option on the left panel. Also, after clicking on the **Site** option in the left panel, the list of configured sites will be displayed in the **Site List** table on the main page.

Click the button to add a new site.



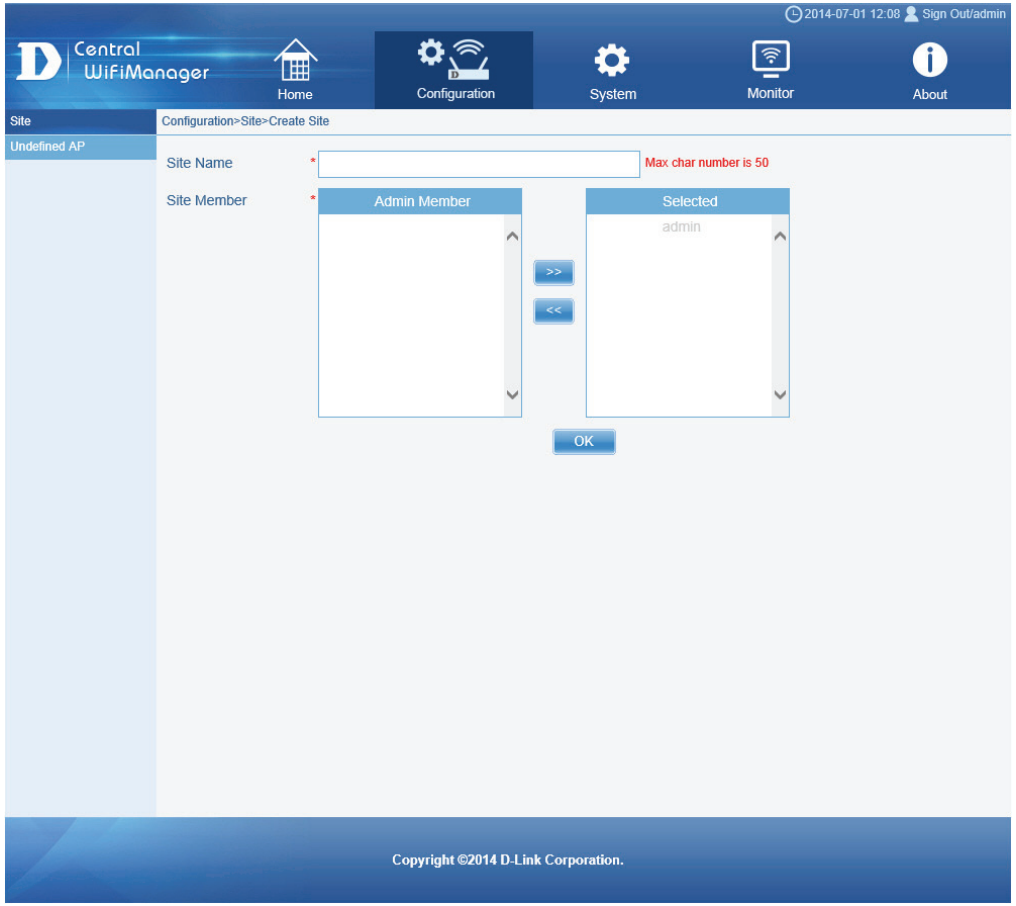
CWM Configuration | Configuration | Site | Create Site

After clicking the button to add a new site, the following page will be available. On this page, users can create sites and also assign member accounts to each site.

The following parameters can be configured:

Parameter	Description
Site Name	Enter the new site's name here. This name can be up to 50 characters long.
Site Member	Select the member accounts that will be added to this site in the left box and click **>>** to add them to the **Selected** list in the right box. To remove a member account from the selected list, select it and click **<<** to remove the account.

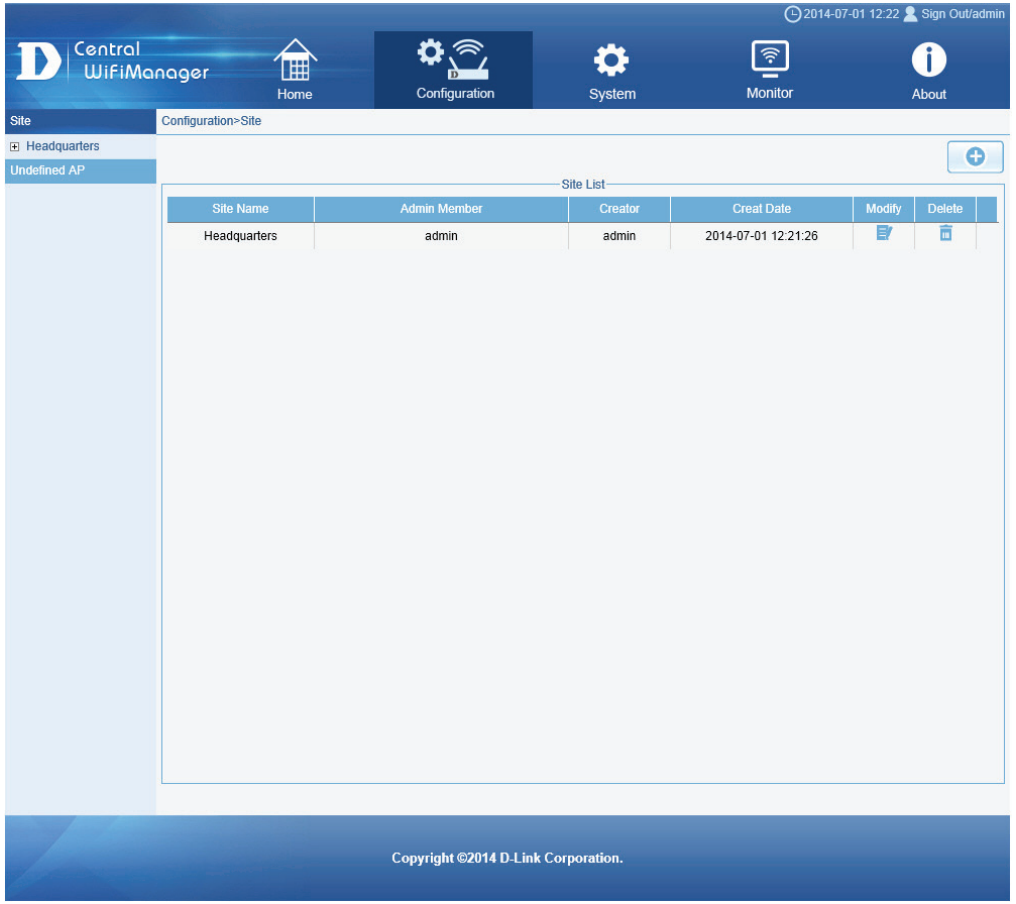
Click the **OK** button to create the new site.



CWM Configuration | Configuration | Site

After creating a new site, it will be displayed in the **Site List** table. In this example, we created a site called **Headquarters**.

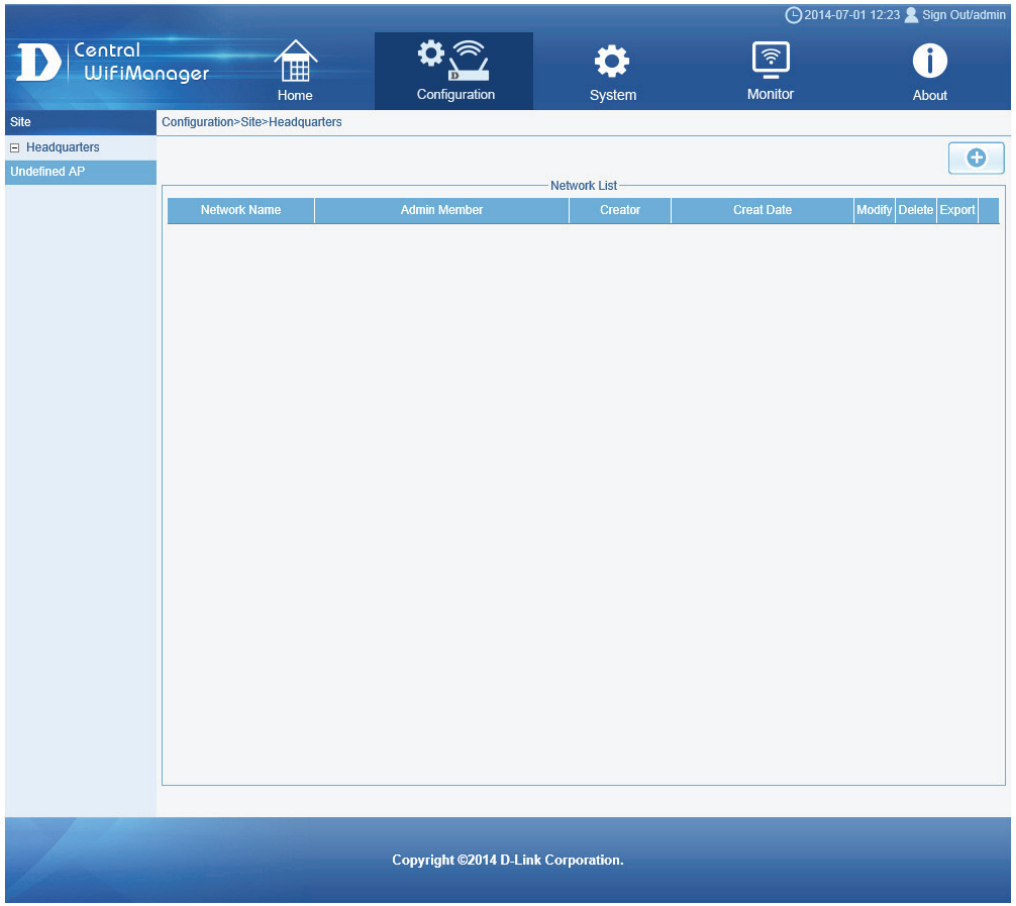
Click the button to add another site.
Click the icon to modify an existing site.
Click the icon to delete an existing site.



CWM Configuration | Configuration | Site | Network

After clicking on the site link called **Headquarters**, in the left panel, we can see the list of networks that have been created for the site in the **Network List** table on the main page.

Click the button to add a new network for this site.



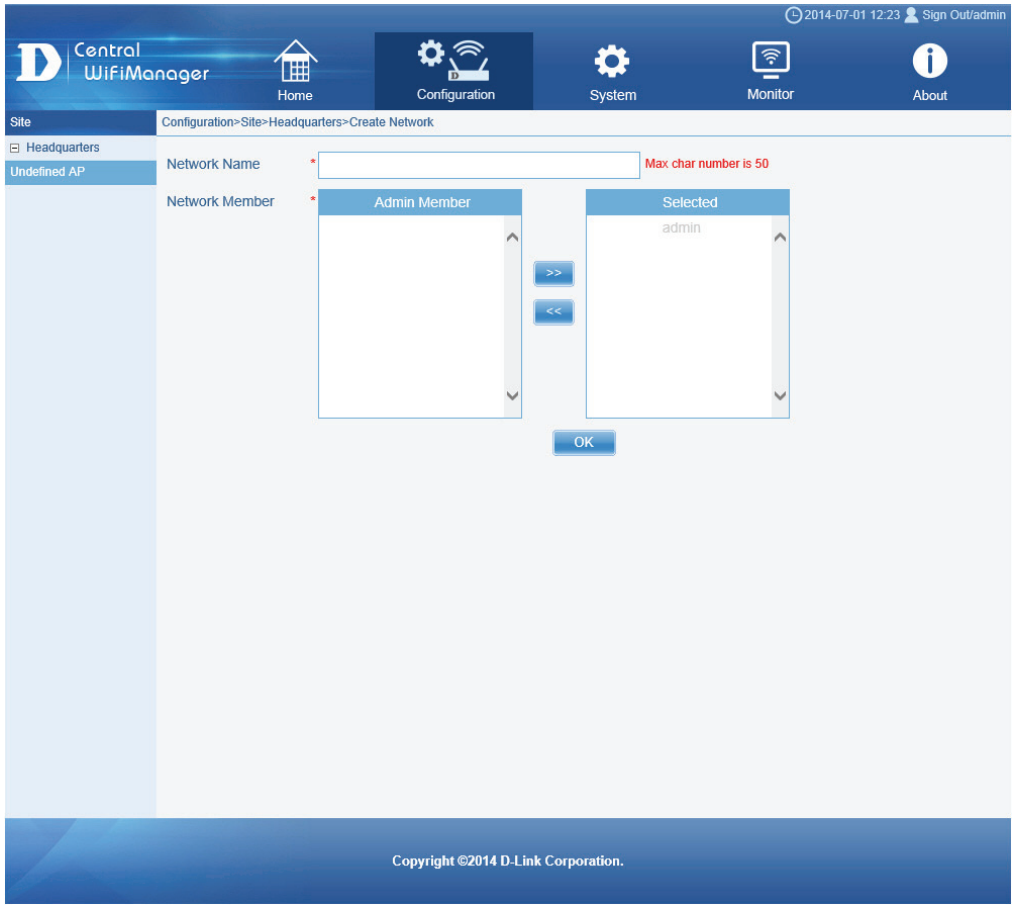
CWM Configuration | Configuration | Site | Network | **Create Network**

After clicking the ⊕ button to add a new network, the following page will be available. On this page, users can create networks and also assign member accounts to each network.

The following parameters can be configured:

Parameter	Description
Network Name	Enter the new network's name here. This name can be up to 50 characters long.
Network Member	Select the member accounts that will be added to this network in the left box and click **>>** to add them to the **Selected** list in the right box. To remove a member account from the selected list, select it and click **<<** to remove the account.

Click the **OK** button to create the new network.

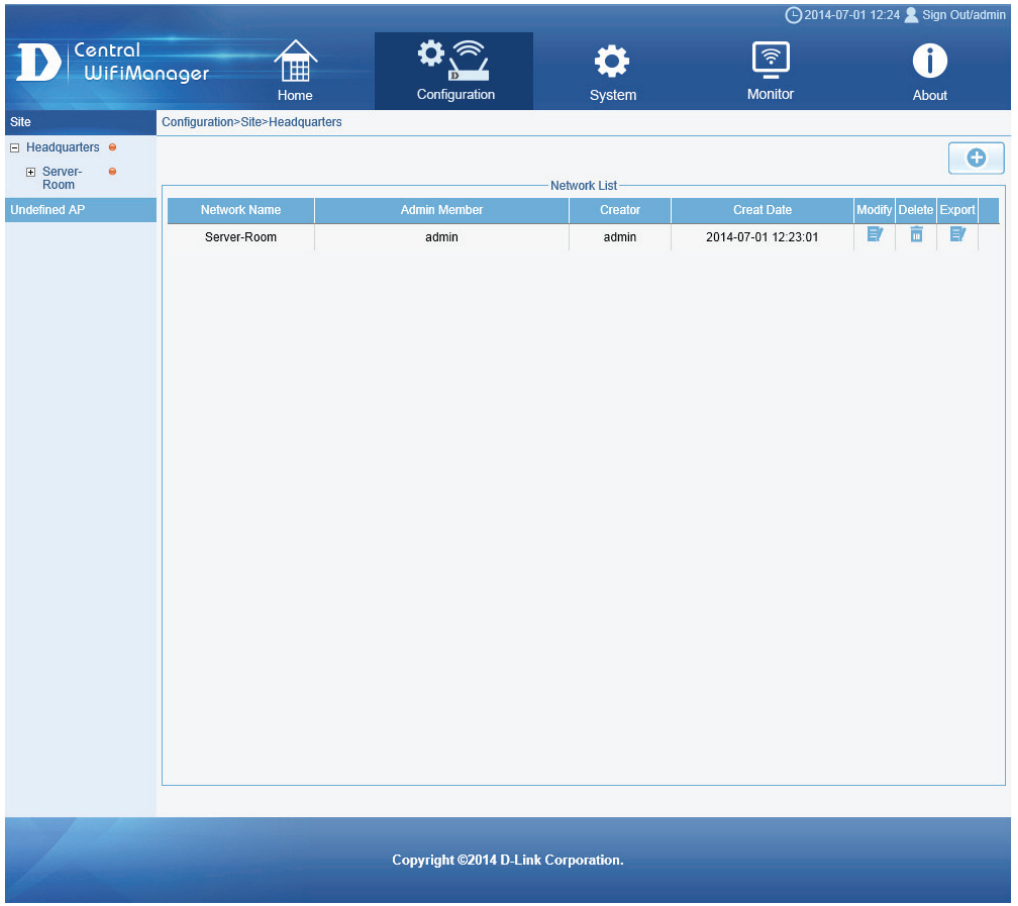


CWM Configuration | Configuration | Site | Network

After creating a new network, it will be displayed in the **Network List** table. In this example, we created a network called **Server-Room**.

Click the button to add another network.
Click the icon to modify an existing network.
Click the icon to delete an existing network.
Click the icon to download the **data file** of this network, that can be **uploaded** to an **access point** to quickly configure an access point to identify with this network.

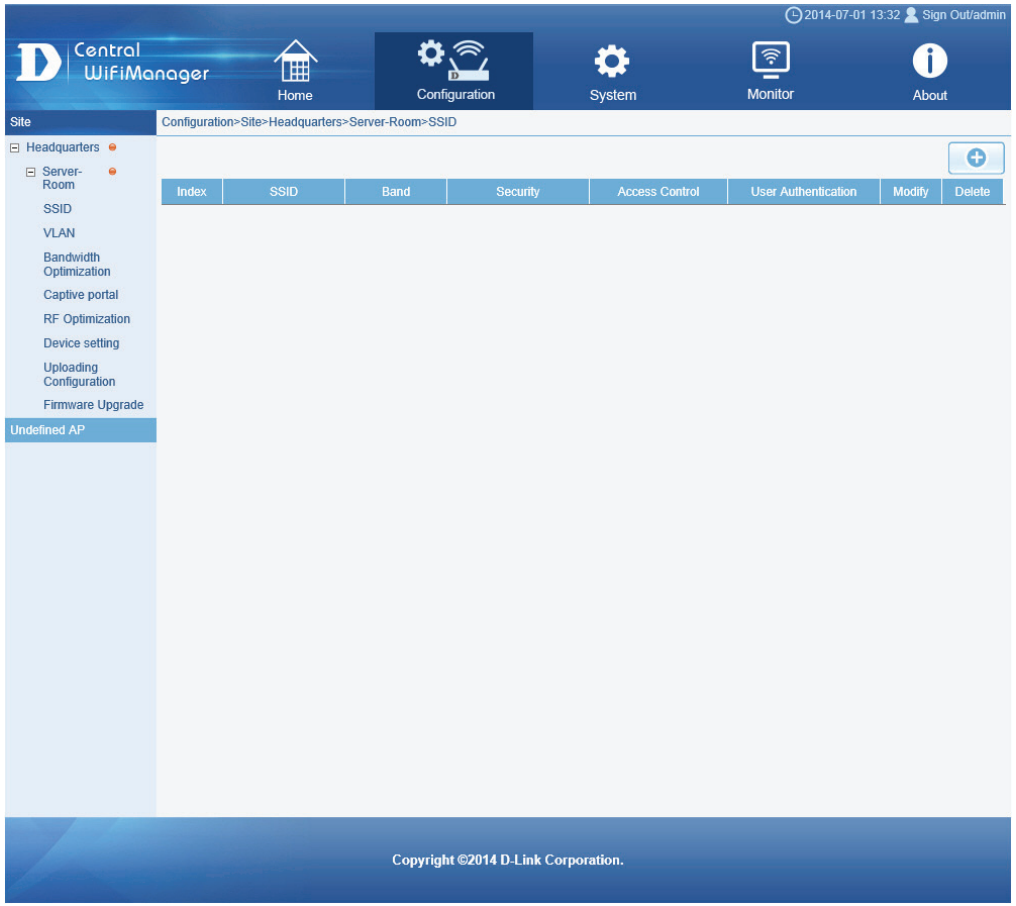
For more information about how to upload the network data file to an access point for seamless network association, refer to "**Access Point Installation Tool**" on page 15.



CWM Configuration | Configuration | Site | Network | SSID

After clicking on the network link called **Server-Room**, in the left panel, a feature rich configuration page is available where users can manually configure settings that will be applied to all access points available in the network selected. On this page we can now create a wireless network profile called **SSID**.

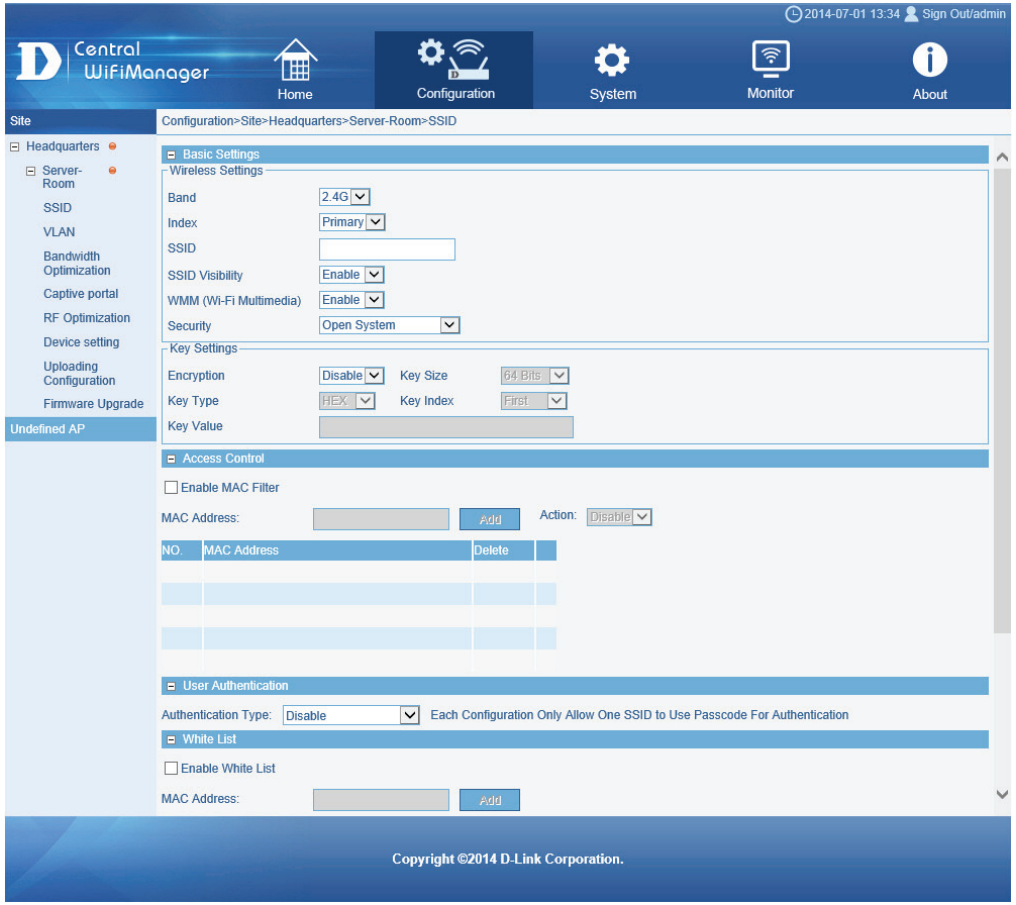
Click the button to add a new SSID.



CWM Configuration | Configuration | Site | Network | SSID | Create SSID

After adding a new SSID, the following page will be available. In the **Basic Settings** section, we can configure the following:

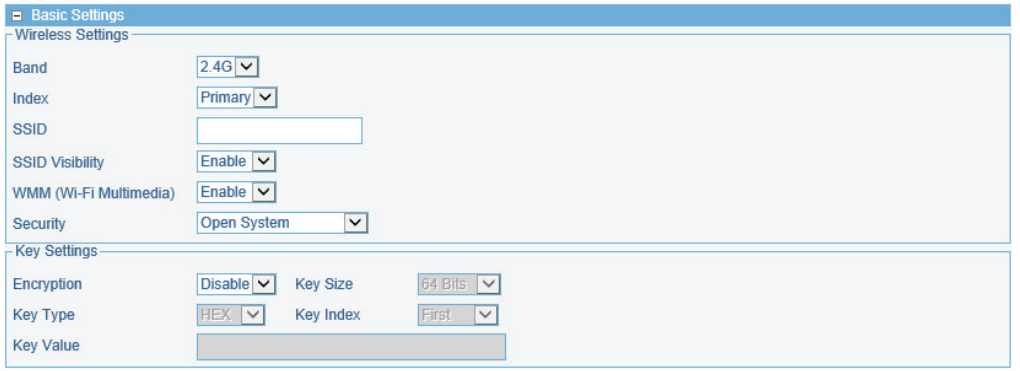
Parameter	Description
Band	Select the wireless frequency band that will be used for this network here. Options to choose from are **2.4G** and **5G**.
Index	Select the SSID index that will be used fore this network here. Options to choose from are **Primary** and **SSID1** to **SSID7**.
SSID	Enter the wireless network name for this network here. This is name is also called the SSID of the wireless network.
SSID Visibility	Select to **Enable** or **Disable** the wireless SSID visibility here.
WMM (Wi-Fi Multimedia)	Select to **Enable** or **Disable** the Wi-Fi multimedia features here.
Security	Select the wireless security that will be used by this wireless network here. Options to choose from are **Open System**, **Shared Key**, **WPA-Personal**, **WPA-Enterprise**, **WPA2-Personal**, **WPA2-Enterprise**, **WPA-Auto-Personal**, and **WPA-Auto-Enterprise**.



In the following sections we'll discuss the wireless security options that are available to networks managed by this application.

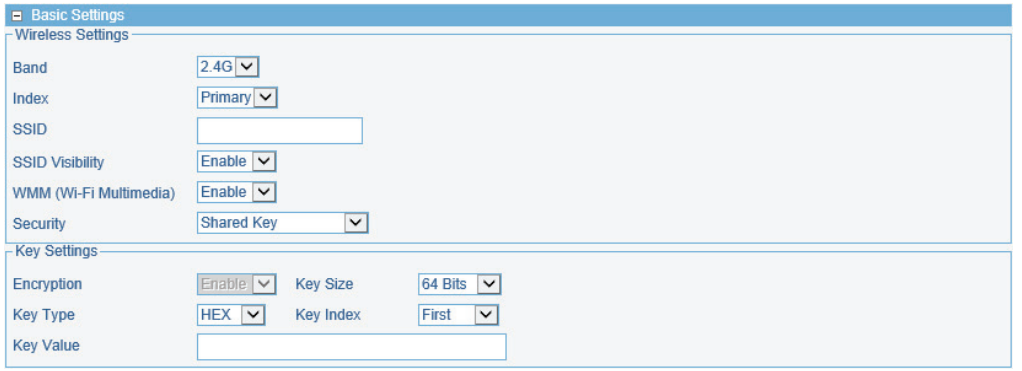
After selecting the WEP **Open System** option as the wireless security method, the following parameters are available for configuration:

Parameter	Description
Encryption	Select this option to **Enable** or **Disable** the WEP Open System encryption method for this network.
Key Size	Select the WEP key size here. Options to choose from are **64 Bits**, **128 Bits**, and **256 Bits**.
Key Type	Select the WEP key type here. Options to choose from are **HEX** and **ASCII**.
Key Index	Select which key in the index of four will be used for this network. Options to choose from are **First**, **Second**, **Third**, and **Fourth**.
Key Value	Enter the open system WEP encryption key here, based on the selections made.



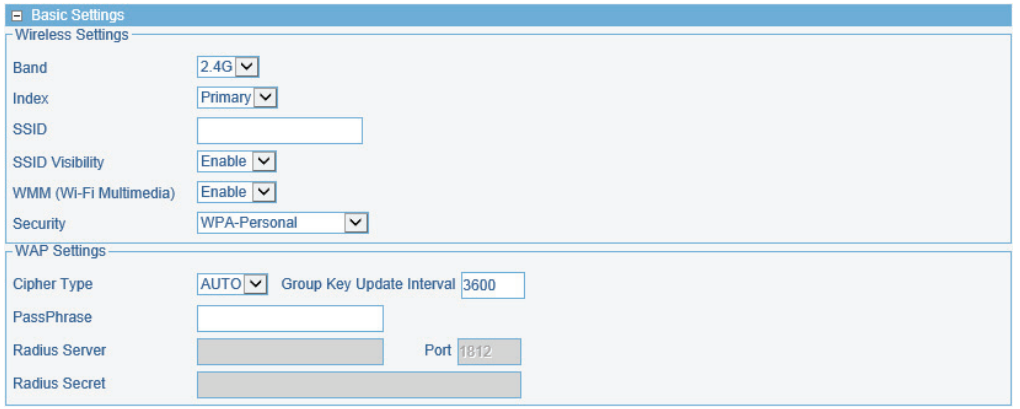
After selecting the WEP **Shared Key** option as the wireless security method, the following parameters are available for configuration:

Parameter	Description
Encryption	Select this option to **Enable** or **Disable** the WEP Shared Key encryption method for this network.
Key Size	Select the WEP key size here. Options to choose from are **64 Bits**, **128 Bits**, and **256 Bits**.
Key Type	Select the WEP key type here. Options to choose from are **HEX** and **ASCII**.
Key Index	Select which key in the index of four will be used for this network. Options to choose from are **First**, **Second**, **Third**, and **Fourth**.
Key Value	Enter the open system WEP encryption key here, based on the selections made.



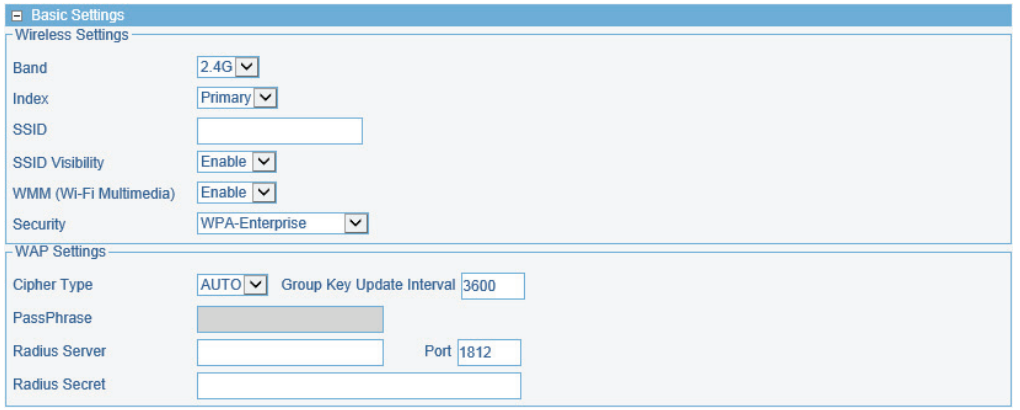
After selecting the **WPA-Personal** option as the wireless security method, the following parameters are available for configuration:

Parameter	Description
Cipher Type	Select the WPA cipher type here. Options to choose from are **Auto**, **AES**, and **TKIP**.
Group Key Update Interval	Enter the WPA group key update interval value here. By default, this value is 3600.
Pass Phrase	Enter the secret pass phrase used here.



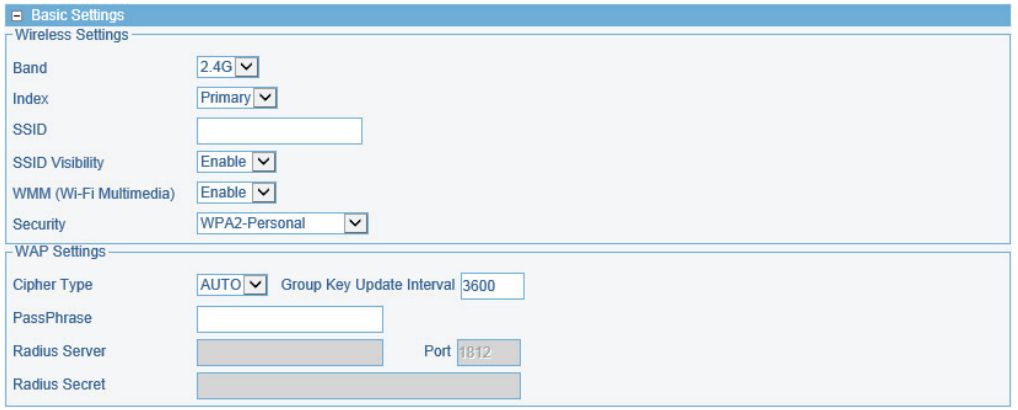
After selecting the **WPA-Enterprise** option as the wireless security method, the following parameters are available for configuration:

Parameter	Description
Cipher Type	Select the WPA cipher type here. Options to choose from are **Auto**, **AES**, and **TKIP**.
Group Key Update Interval	Enter the WPA group key update interval value here. By default, this value is 3600.
RADIUS Server	Enter the RADIUS server's IP address here.
Port	Enter the RADIUS server's port number used here. By default, this port number is 1812.
RADIUS Secret	Enter the RADIUS secret pass phrase used here.



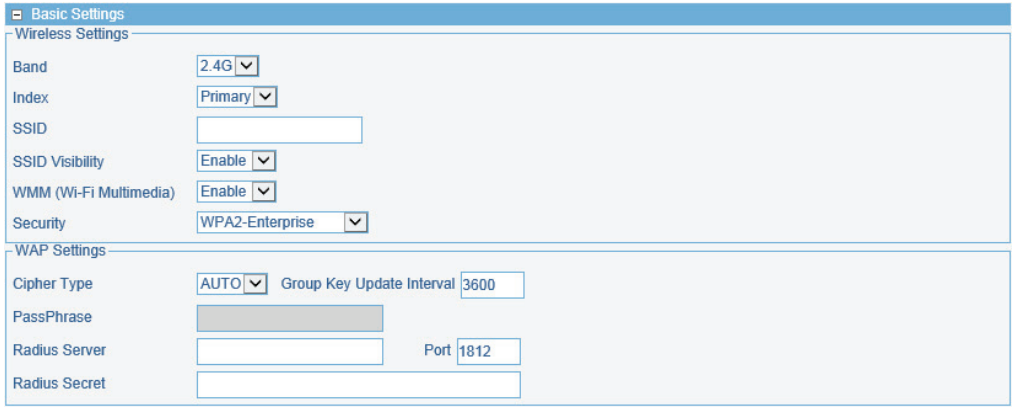
After selecting the **WPA2-Personal** option as the wireless security method, the following parameters are available for configuration:

Parameter	Description
Cipher Type	Select the WPA2 cipher type here. Options to choose from are **Auto**, **AES**, and **TKIP**.
Group Key Update Interval	Enter the WPA2 group key update interval value here. By default, this value is 3600.
Pass Phrase	Enter the secret pass phrase used here.



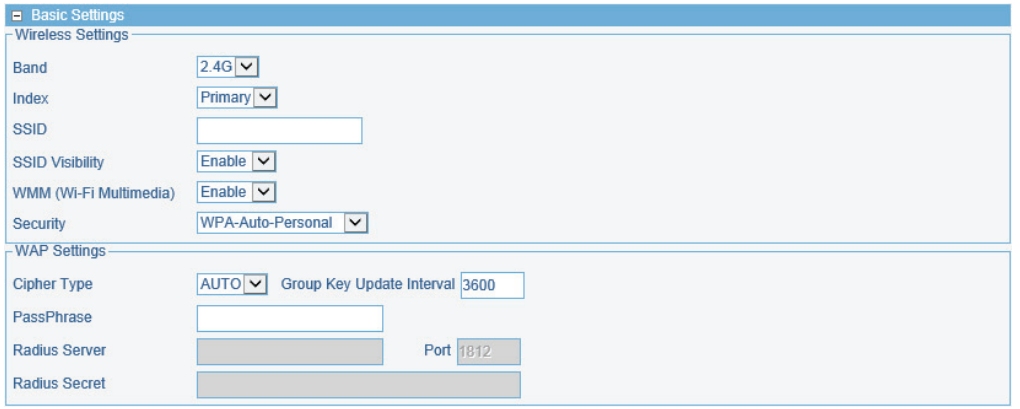
After selecting the **WPA2-Enterprise** option as the wireless security method, the following parameters are available for configuration:

Parameter	Description
Cipher Type	Select the WPA2 cipher type here. Options to choose from are **Auto**, **AES**, and **TKIP**.
Group Key Update Interval	Enter the WPA2 group key update interval value here. By default, this value is 3600.
RADIUS Server	Enter the RADIUS server's IP address here.
Port	Enter the RADIUS server's port number used here. By default, this port number is 1812.
RADIUS Secret	Enter the RADIUS secret pass phrase used here.



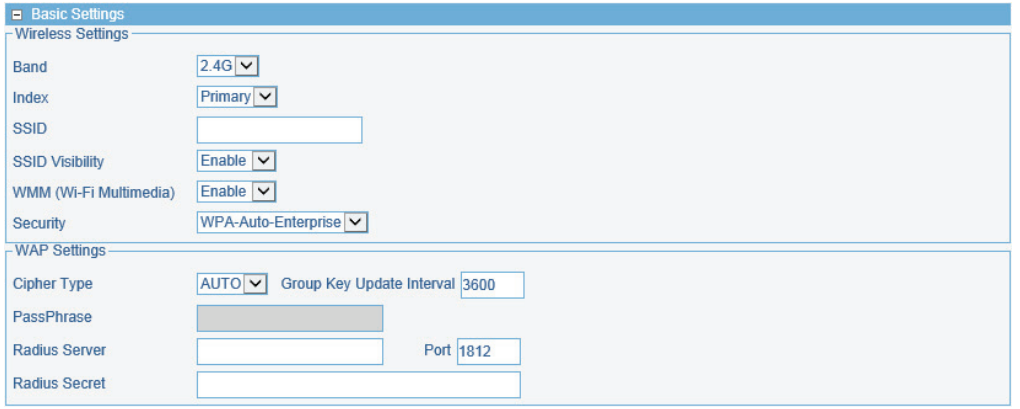
After selecting the **WPA-Auto-Personal** option as the wireless security method, the following parameters are available for configuration:

Parameter	Description
Cipher Type	Select the WPA/WPA2 cipher type here. Options to choose from are **Auto**, **AES**, and **TKIP**.
Group Key Update Interval	Enter the WPA/WPA2 group key update interval value here. By default, this value is 3600.
Pass Phrase	Enter the secret pass phrase used here.



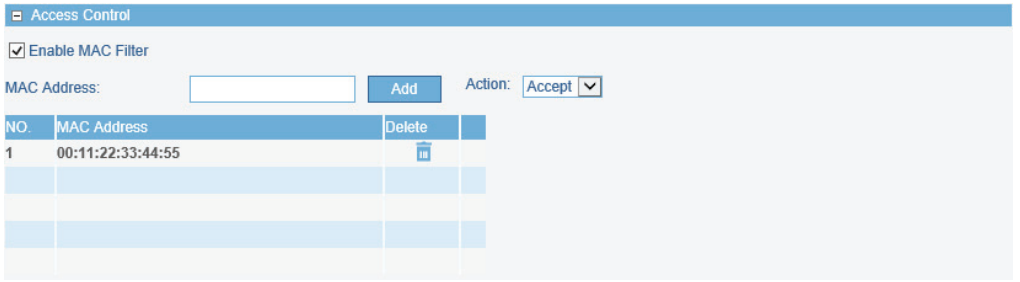
After selecting the **WPA-Auto-Enterprise** option as the wireless security method, the following parameters are available for configuration:

Parameter	Description
Cipher Type	Select the WPA/WPA2 cipher type here. Options to choose from are **Auto**, **AES**, and **TKIP**.
Group Key Update Interval	Enter the WPA/WPA2 group key update interval value here. By default, this value is 3600.
RADIUS Server	Enter the RADIUS server's IP address here.
Port	Enter the RADIUS server's port number used here. By default, this port number is 1812.
RADIUS Secret	Enter the RADIUS secret pass phrase used here.



In the **Access Control** section we can configure which network devices can have access to the network or not by specifying the MAC of the accepted or rejected devices. The following parameters can be configured.

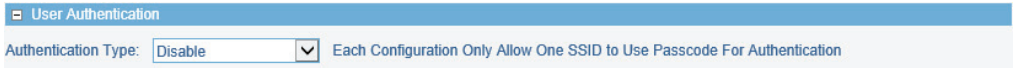
Parameter	Description
Enable MAC Filter	Select this option to enable the MAC filtering feature.
MAC Address	Enter the MAC address of the networking device that will be used for this configuration here.
Action	Select the action that will be applied to the networking device. Option to choose from are **Disable**, **Accept** and **Reject**.



A list of configured entries will be displayed in the table.
Click the icon to remove a specific entry.

In the **User Authentication** section we can configure the authentication method that will be applied to all the wireless clients that connect to access point in this network. The following parameters can be configured.

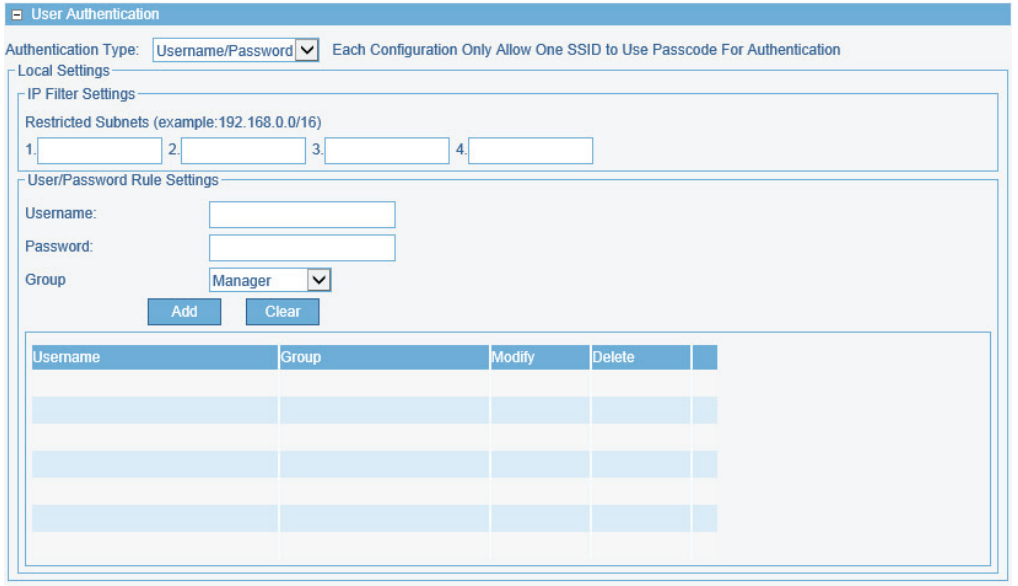
Parameter	Description
Authentication Type	Select the authentication type that will be applied to the wireless clients in this network. Options to choose from are **Disable**, **Username/Password**, **Remote RADIUS**, **LDAP**, **POP3** and **Passcode**. After selecting **Disable** as the authentication type, this feature will be disabled.


User Authentication
Authentication Type:
Disable
Each Configuration Only Allow One SSID to Use Passcode For Authentication

CWM Configuration | Configuration | Site | Network | SSID | Create SSID

After selecting **Username/Password** as the **Authentication Type**, we can apply local authentication to each wireless client in this network. Local authentication means that no external server is needed to help with the authentication process. Authentication is applied based on restricted subnets, username and password authentication based on the accounts created here and the group that they belong to. The following parameters can be configured.

Parameter	Description
Restricted Subnets	If any restricted subnets exist on the network that wireless should not be able to access, enter those network addresses in the spaces provided. Up to four different subnets can be restricted. For example 192.168.0.0/16. Note that the CDIR notation is used to indicate the subnet mask of the subnet. Users in the guest group will not be able to access these restricted subnets. In the example the CDIR notation of 16 is used, which is equivalent to the subnet mask of 255.255.0.0. This means that IP addresses from 192.168.0.0 to 192.168.255.255 will be restricted.
Username	Enter the username that the wireless clients should use here.
Password	Enter the password that the wireless clients should use here.
Group	Select the group that the user account belongs to here. Different groups will be have different access privileges given to the user account created here.



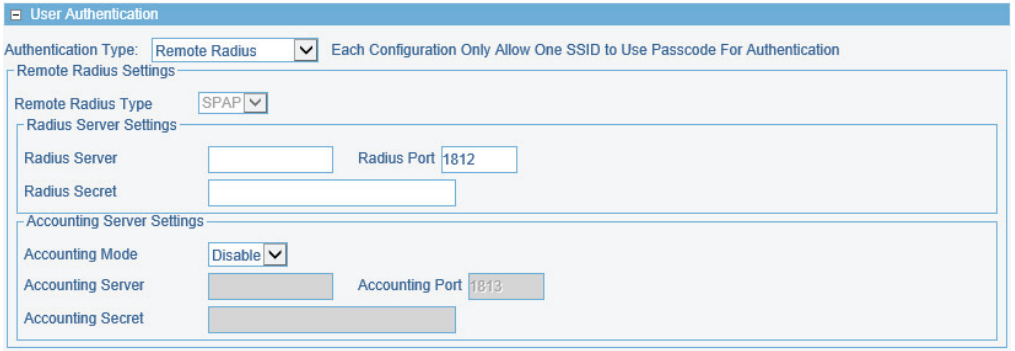
A list of configured user accounts will be displayed in the table.

Click the icon to modify an existing account.
Click the icon to delete an existing account.

CWM Configuration | Configuration | Site | Network | SSID | **Create SSID**

After selecting **Remote RADIUS** as the **Authentication Type**, we can configure access points in this network to act as authenticator devices that will communicate and relay authentication messages to an additional RADIUS server installed in the network. The following parameters can be configured.

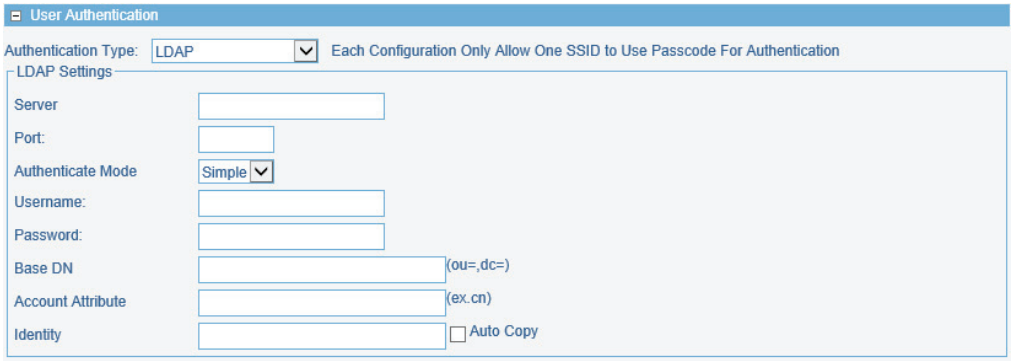
Parameter	Description
Remote RADIUS Type	This field will display the remote RADIUS server type that can be used. The remote RADIUS server type is SPAP.
RADIUS Server	Enter the RADIUS server's IP address here.
RADIUS Port	Enter the RADIUS server's port number used here. By default this value is 1812.
RADIUS Secret	Enter the RADIUS server secret here.
Accounting Mode	Select to **Enable** or **Disable** the RADIUS server accounting feature here.
Accounting Server	Enter the RADIUS accounting server's IP address here.
Accounting Port	Enter the RADIUS accounting server's port number here. By default this value is 1813.
Accounting Secret	Enter the RADIUS accounting server's secret here.



CWM Configuration | Configuration | Site | Network | SSID | Create SSID

After selecting **LDAP** as the **Authentication Type**, we can configure access points to use an additional LDAP server to handle user authentication in this network. The following parameters can be configured.

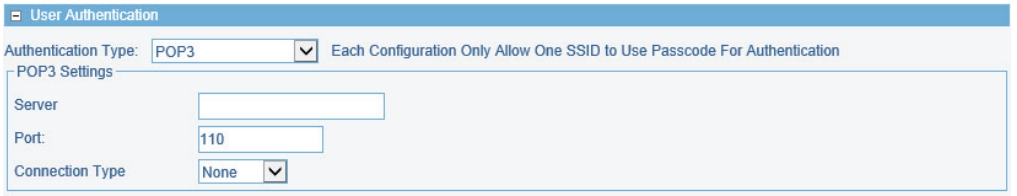
Parameter	Description
Server	Enter the LDAP server's IP address here.
Port	Enter the LDAP server's port number used here.
Authenticate Mode	Select the authentication mode that will be used here. Options to choose from are **Simple** and **TLS**.
Username	Enter the administrator's username here that will be able to access and search the LDAP database.
Password	Enter the administrator's password here that will be able to access and search the LDAP database.
Base DN	Enter the base domain name of the LDAP database here. For example, **cn=users, dc=test, dc=com** means that the wireless client is a member of the group **users** in the domain **test.com**.



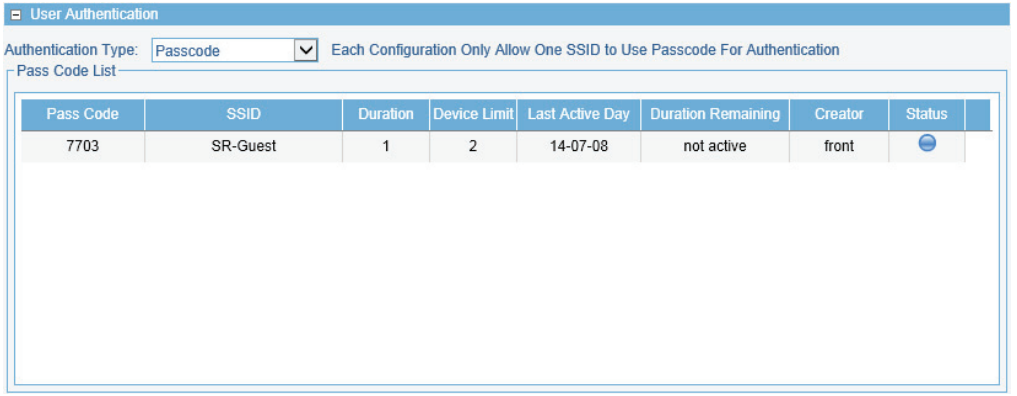
Account Attribute	Enter the attribute for the account here. For example, **cn** is used for Windows Server.
Identity	Enter the name of the administrator here. For example, **cn=Administrator, cn=users, dc=test, dc=com** means for Windows Server, if the administrator is a member of wireless client, it is also a member of the group **users** in the domain **test.com**. Alternatively select the **Auto Copy** option to automatically generate and insert the name of the administrator here based on the **Base DN** and **Account Attribute** strings entered.

After selecting **POP3** as the **Authentication Type**, we can configure access points to use an additional POP3 server to handle user authentication in this network. The following parameters can be configured.

Parameter	Description
Server	Enter the POP3 server's IP address here.
Port	Enter the POP3 server's port number used here. By default this port number is 110. For the SSL/TLS connection type this value is 995 by default.
Connection Type	Select the POP3 connection type here. Options to choose from are **None** and **SSL/TLS**.



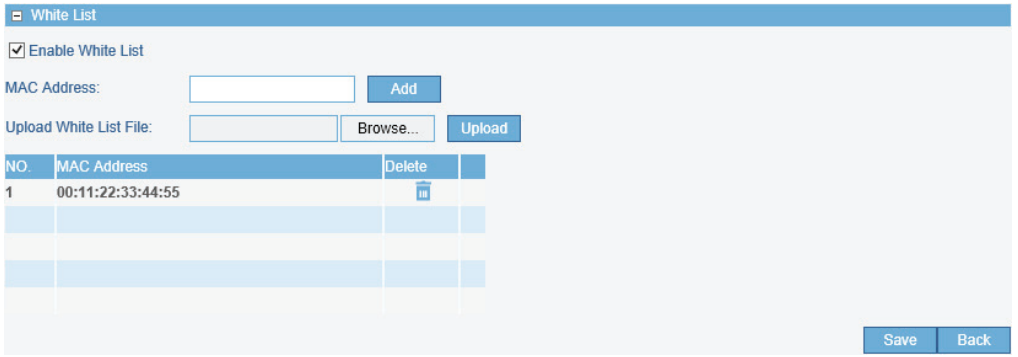
After selecting **Passcode** as the **Authentication Type**, we can view the following section. In this table configured front desk user accounts that have been assigned to this network and have already generated a pass code from the Web login page, will be displayed.



For more information about creating or configuring user accounts refer to "**Create User Account**" on page 63.
For more information about front desk user accounts refer to "**Appendix A - Front Desk Staff & User Access**" on page 95.

In the **White List** section we can configure what network devices are allowed to connect to this network by specifying the MAC address of those network devices. The following parameters can be configured.

Parameter	Description
Enable White List	Select this option to enable the white list feature.
MAC Address	Enter the MAC address of the networking device that will be allowed to connect to this network here. Click **Add** to then add this MAC address to the white list table.
Upload White List File	To upload a white list file, click **Browse** and navigate to the white list file, saved on the computer, and then click **Upload**.

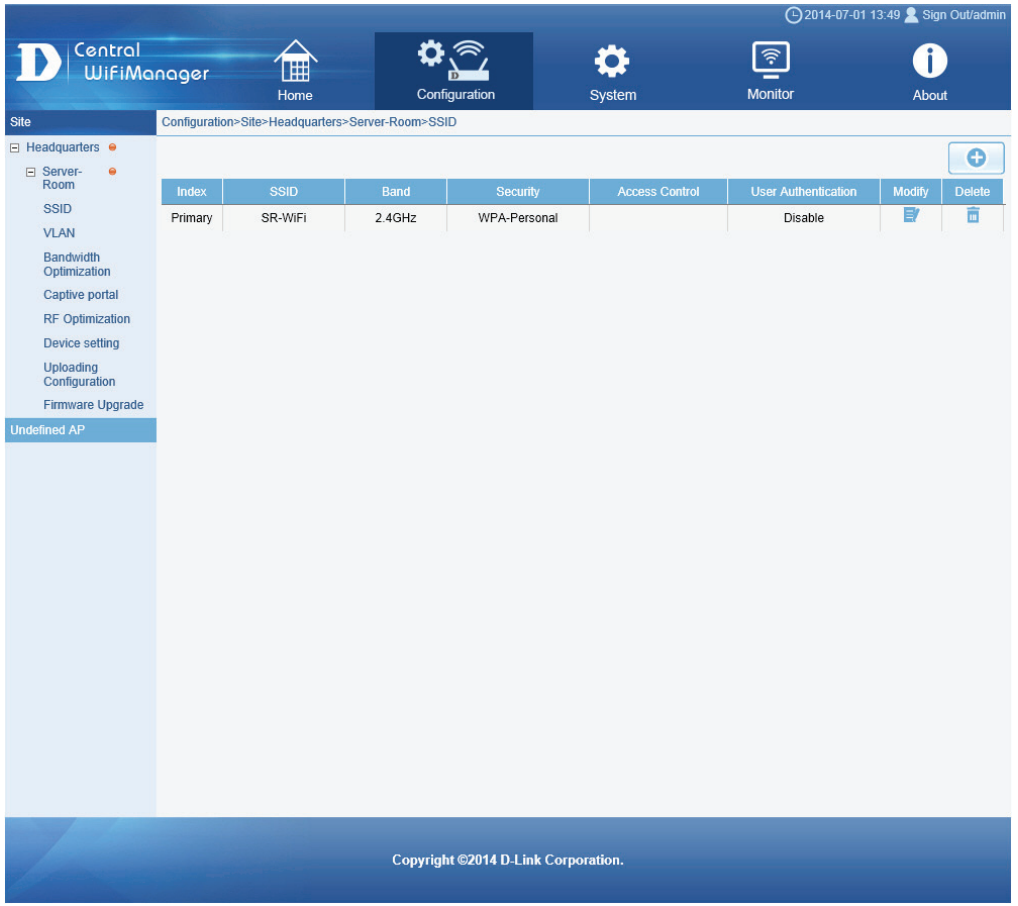


Click the **Save** button to accept the changes made.
Click the **Back** button to discard the changes made and return to the main page.

CWM Configuration | Configuration | Site | Network | SSID

After creating a new SSID, it will be displayed in the table. In this example, we created an SSID called **SR-WiFi**.

Click the button to add another new SSID.
Click the icon to modify an existing SSID.
Click the icon to delete an existing SSID.



CWM Configuration | Configuration | Site | Network | VLAN

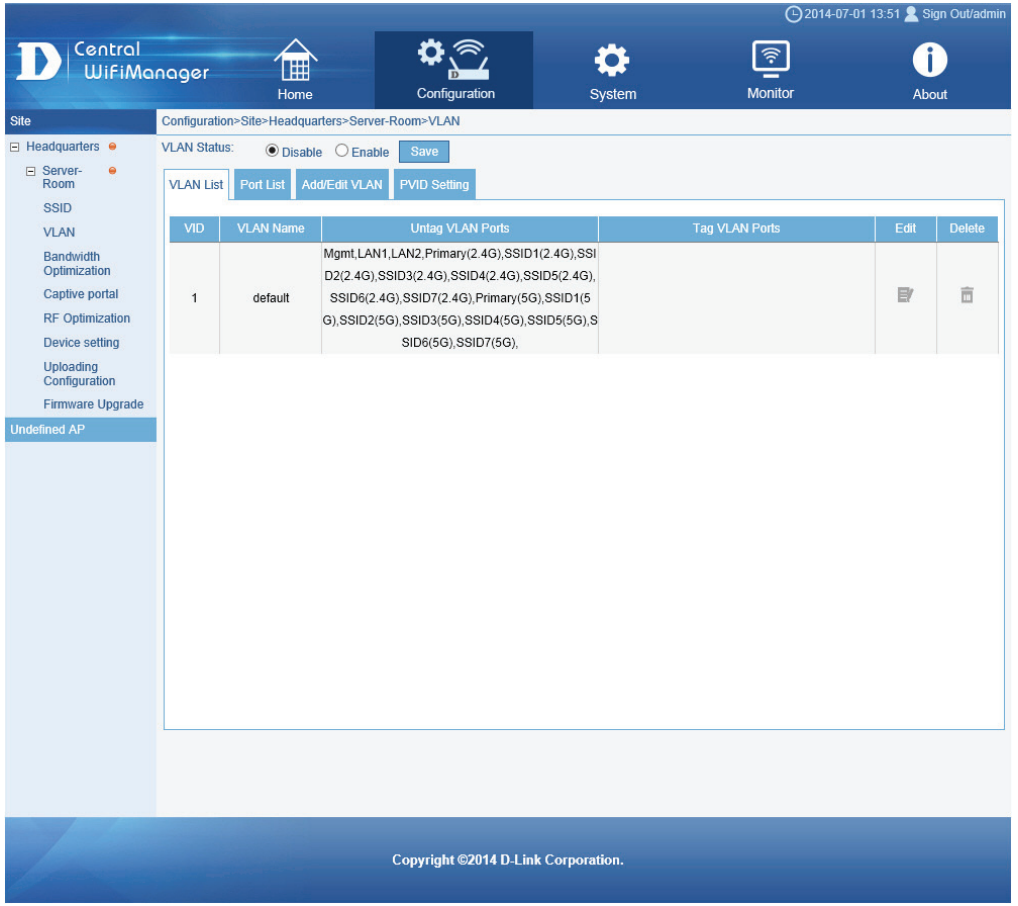
After creating a network, additional options will be available in the left panel. These options include **VLAN**, **Bandwidth Optimization**, **Captive Portal**, **RF Optimization**, **Device settings**, **Uploading Configuration** and **Firmware Upgrade**.

In the following sections, we'll discuss these additional settings in more detail.

Before the tabs, we can configure the following parameter.

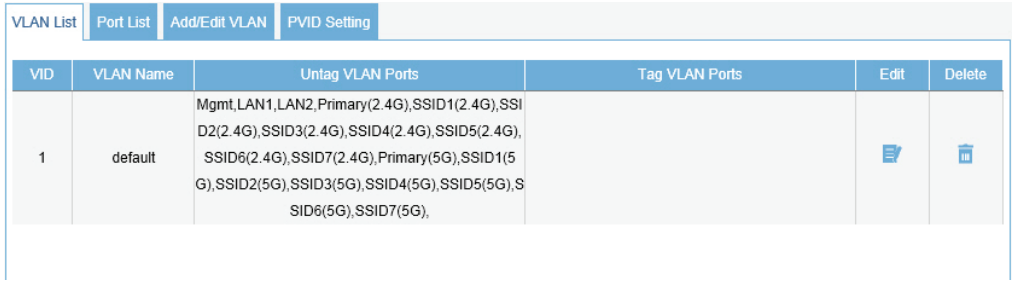
Parameter	Description
VLAN Status	Select to **Enable** or **Disable** the VLAN feature here.

Click the **Save** button to accept the changes made.



CWM Configuration | Configuration | Site | Network | VLAN

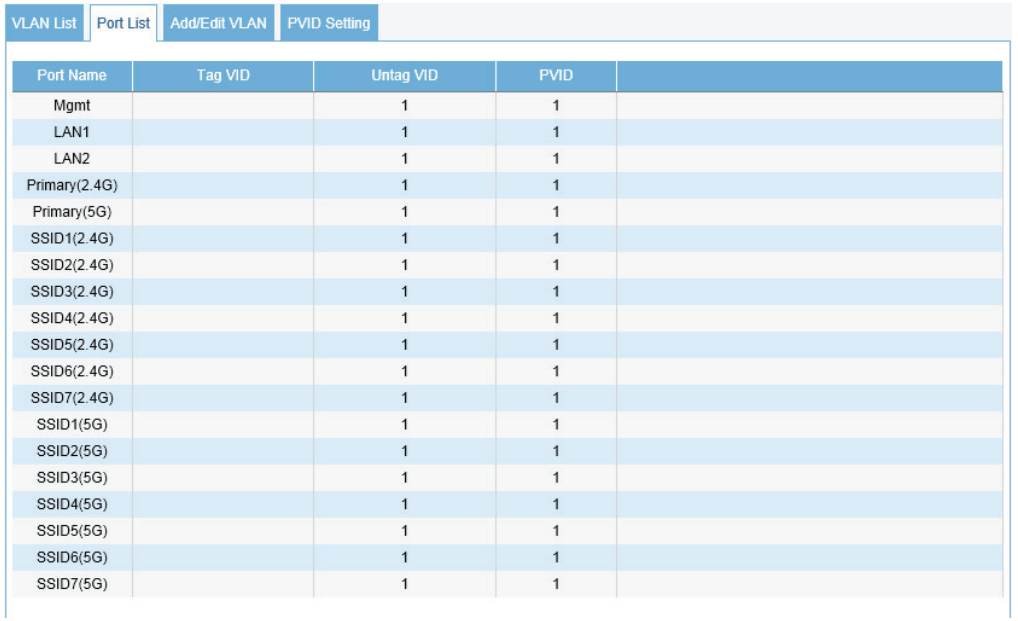
After clicking on **VLAN** in the left panel, the following page will be available. On this page we can view, create and configure Virtual LANs (VLANs) that will be managed by the access point in this network.



In the **VLAN List** tab, a list of created VLANs will be displayed.

Click the **Edit** icon to modify an existing VLAN.
Click the **Delete** icon to remove an existing VLAN.

In the **Port List** tab, a list of ports will be displayed. These ports are all the ports that are available on the access points in the network.



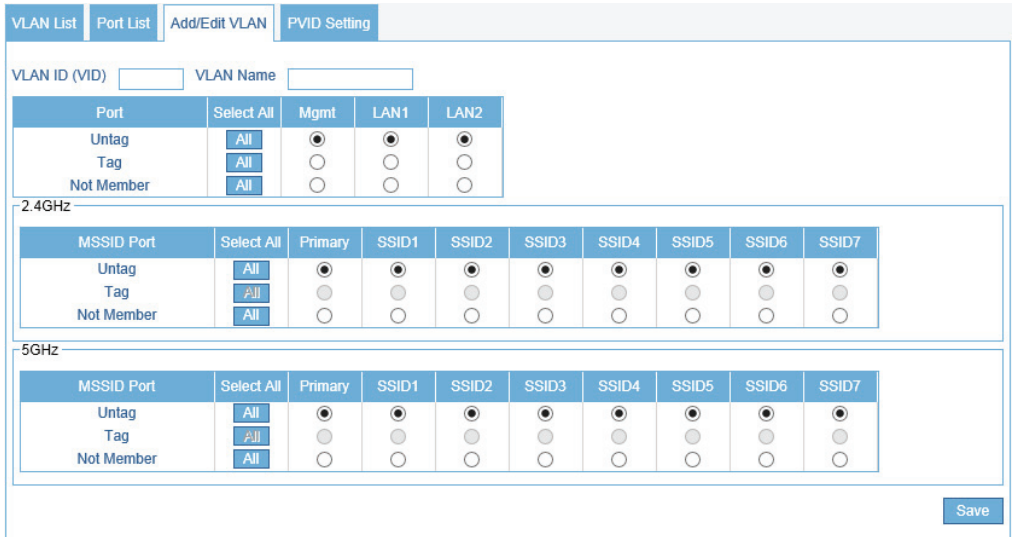
In the columns next to the **Port Name** entries, the VLAN ID number of the VLAN that the port belongs to will be displayed. The column location of the number will indicate if the port is a tagged member (**Tag VID**) or an untagged member (**Untag VID**) of the VLAN. In the last column the **PVID** number of that specific port will be displayed.

CWM Configuration | Configuration | Site | Network | **VLAN**

In the **Add/Edit VLAN** tab, we can create a new VLAN and assign the port membership to each port in that VLAN. After clicking the **Modify** icon in the **VLAN List** tab, we will be re-directed to this tab to modify an existing VLAN.

The following parameters can be configured.

Parameter	Description
VLAN ID (VID)	Enter the VLAN's ID here.
VLAN Name	Enter the VLAN's name here.
Port	Select the port membership option for each port in this column. Port in VLAN in this network can either be untagged (**Untag**) members, tagged (**Tag**), or non-members (**Not Member**).
Select All	Which this button is clicked, all the ports in the table will be changed to either be **Untag**, **Tag** or **Not Member**.
Mgmt	This is the management port on access points.
LAN1 ~ LAN2	This is the LAN ports on access points. If the access point has only one LAN port, it will be LAN1.
Primary	This is the primary WLAN SSID on access points in this network.
SSID1 ~ SSID7	This is the secondary WLAN SSIDs on access points in this network.



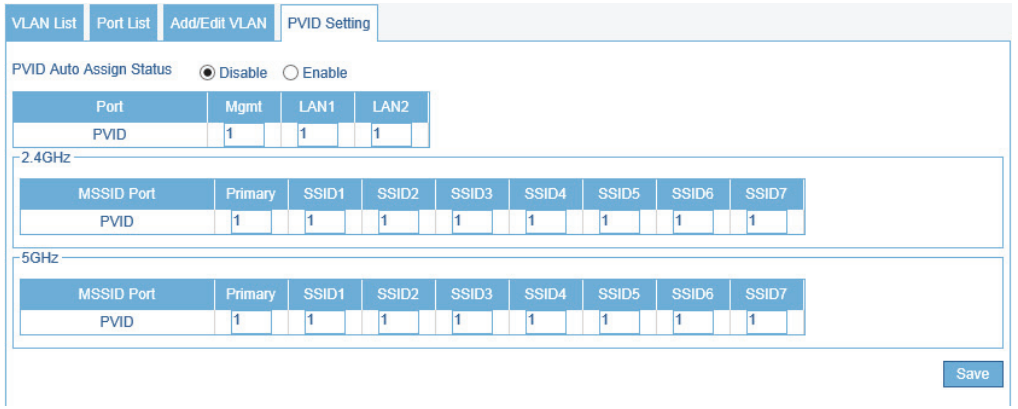
Click the **Save** button to accept the changes made.

CWM Configuration | Configuration | Site | Network | **VLAN**

In the **PVID Setting** tab, we can view and configure the Port VLAN Identifier (PVID) settings for access points and wireless client in this network.

The following parameters can be configured.

Parameter	Description
PVID Auto Assign Status	Select to **Enable** or **Disable** the PVID automatic assign status feature here.
PVID	Enter the PVID number in the spaces provided for the corresponding ports.
Mgmt	This is the management port on access points.
LAN1 ~ LAN2	This is the LAN ports on access points. If the access point has only one LAN port, it will be LAN1.
Primary	This is the primary WLAN SSID on access points in this network.
SSID1 ~ SSID7	This is the secondary WLAN SSIDs on access points in this network.



Click the **Save** button to accept the changes made.

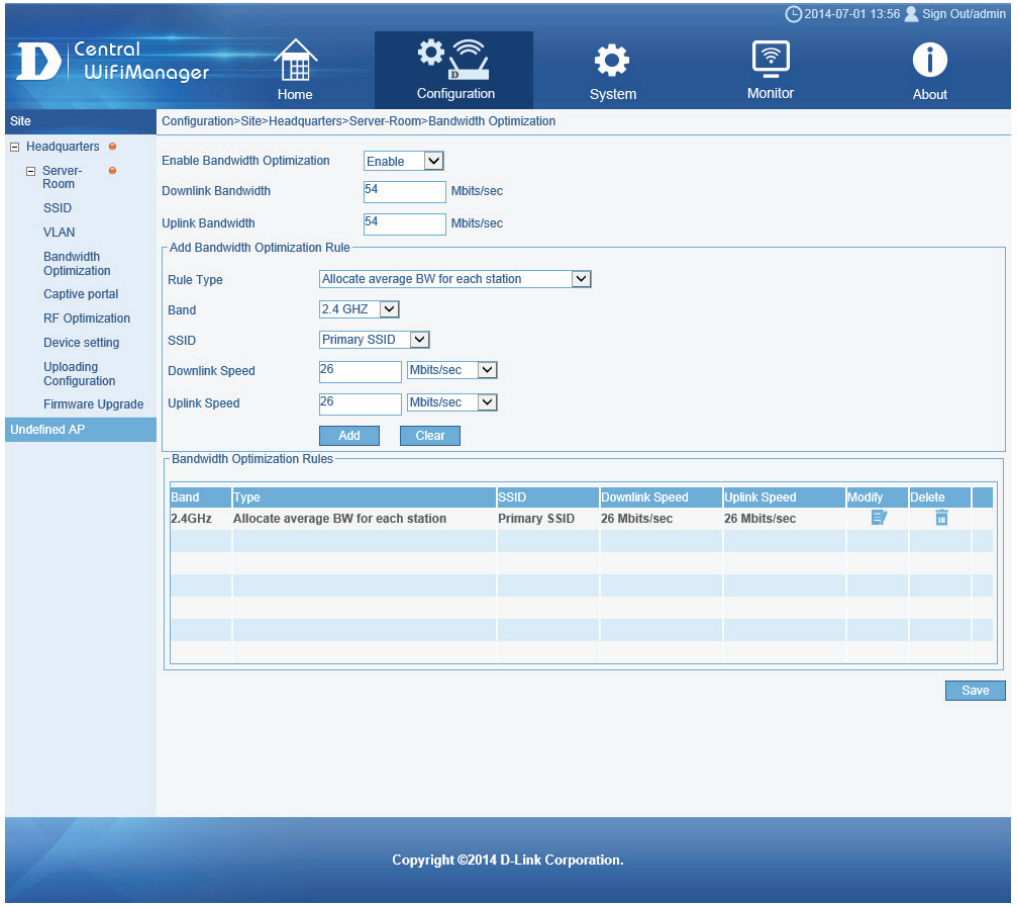
CWM Configuration | Configuration | Site | Network | **Bandwidth Optimization**

After clicking on **Bandwidth Optimization** in the left panel, the following page will be available. On this page we can view and configure the bandwidth settings for access points in this network.

The following parameters can be configured.

Parameter	Description
Enable Bandwidth Optimization	Select to **Enable** or **Disable** the bandwidth optimization feature here.
Downlink Bandwidth	Enter the total downlink bandwidth speed for access points in this network here. This value is in Mbits/sec.
Uplink Bandwidth	Enter the total uplink bandwidth speed for access points in this network here. This value is in Mbits/sec.
Rule Type	Select the type of rule that will be create or modified here. Options to choose from are the following: • **Allocate average BW for each station**: The AP will distribute average bandwidth for each client. • **Allocate maximum BW for each station**: Specify the maximum bandwidth for each connected client. Reserve certain bandwidth for future clients. • **Allocate different BW for 11a/b/g/n station**: The weight of 802.11b/g/n and 802.11a/n clients are 10%/20%/70% and 20%/80%. The AP will distribute different bandwidth for 802.11a/b/g/n clients. • **Allocate specific BW for SSID**: All clients share the total bandwidth.
Band	Select the wireless frequency band that will be used in this rule here. Options to choose from are **2.4Ghz** and **5GHz**.
SSID	Select which SSID will be used in this rule here. Options to choose from are **Primary SSID** and **SSID1** to **SSID7**.
Downlink Speed	Enter the downlink speed value that will be assigned to either each station or to the specified SSID here. This value can either be in **Mbits/sec** or **Kbits/sec**.
Uplink Speed	Enter the uplink speed value that will be assigned to either each station or to the specified SSID here. This value can either be in **Mbits/sec** or **Kbits/sec**.

Click the **Add** button to add the new rule to the list of **Bandwidth Optimization Rules**.



Click the **Clear** button to clear out all the information entered in the fields.
Click the **Save** button to accept the changes made.

Click the icon to modify an existing rule.
Click the icon to delete an existing rule.

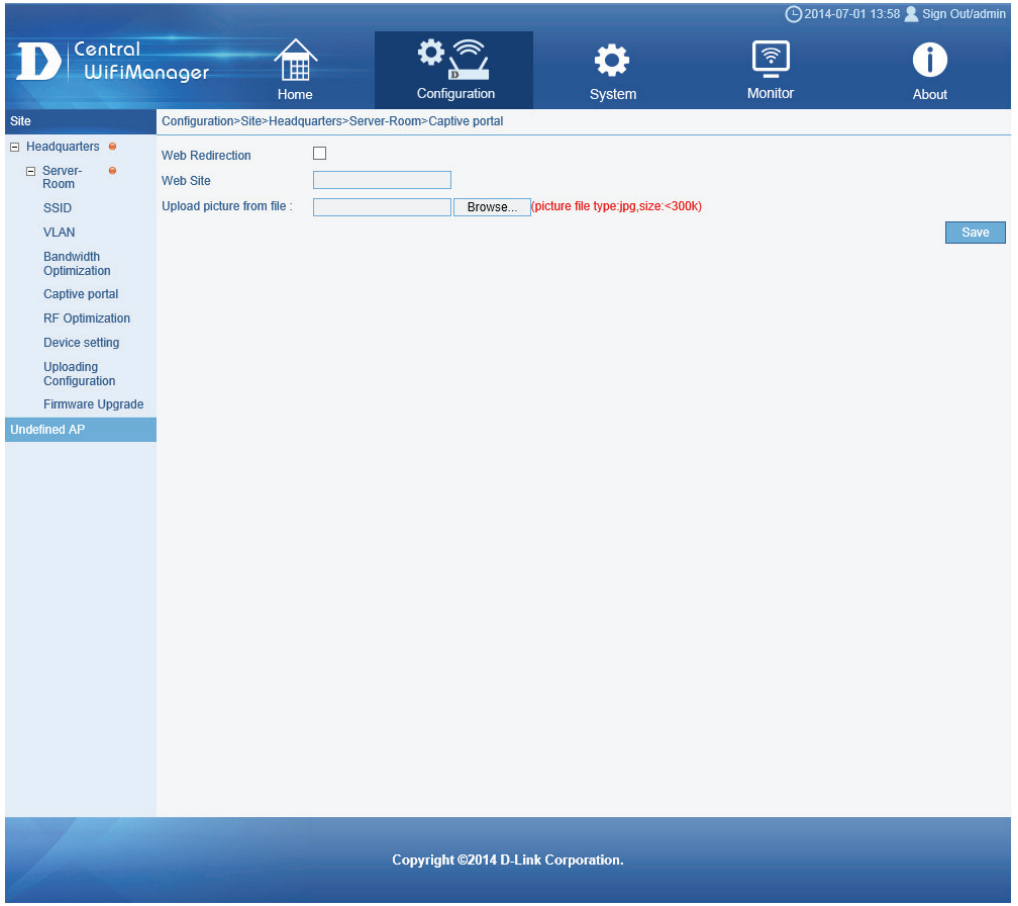
CWM Configuration | Configuration | Site | Network | **Captive Portal**

After clicking on **Captive Portal** in the left panel, the following page will be available. On this page we can view and configure the captive portal settings for access points and wireless clients in this network.

The following parameters can be configured.

Parameter	Description
Web Redirection	Select this option to enable the web redirection feature.
Web Site	Enter the redirection web site's URL address here
Upload picture from file	To upload and use a picture file, click on **Browse** and navigate to the image file located on the computer.

Click the **Save** button to accept the changes made.



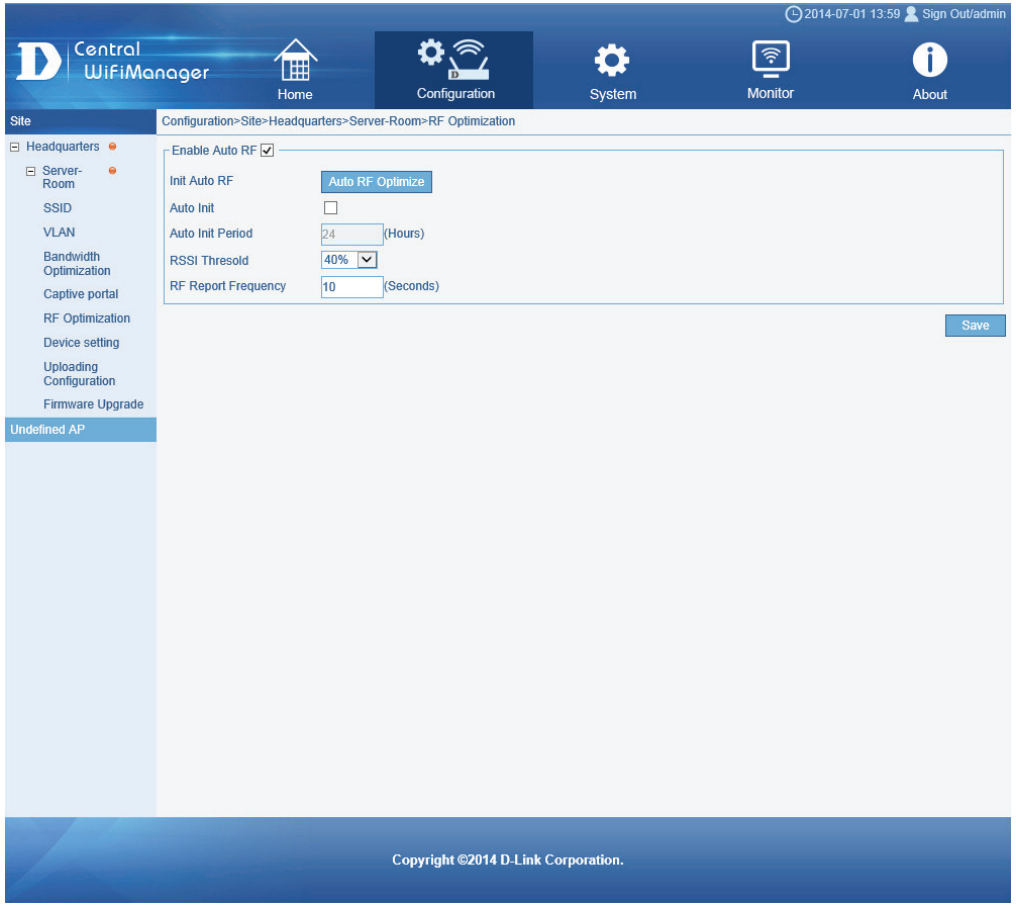
CWM Configuration | Configuration | Site | Network | **Bandwidth optimization**

After clicking on **Bandwidth optimization** in the left panel, the following page will be available. On this page we can view and optimize the Radio Frequency (RF) used on the access points in this network.

The following parameters can be configured.

Parameter	Description
Enable Auto RF	Select this option to enable the RF optimization feature.
Init Auto RF	Click the **Auto RF Optimize** button to manually initiate the automatic RF optimization feature. The AP will automatically select the best channel.
Auto Init	Select this option to run the RF optimization feature periodically based on the period entered. After the initiation period has expired, the AP will automatically select the best channel.
Auto Init Period	After enabling the **Auto Init** option, enter the automatic initiation period value in hours here.
RSSI Threshold	Select the RSSI threshold value for this network here. This value is between **10%** and **100%** in increments of 10%. The AP will adjust its channel or power when, after a scan, it detected APs in the network with a lower RSSI than the threshold specified.
RF Report Frequency	Enter the frequency value, in seconds, at which an RF report will be generated. The AP might adjust its channel or power at the frequency specified.

Click the **Save** button to accept the changes made.



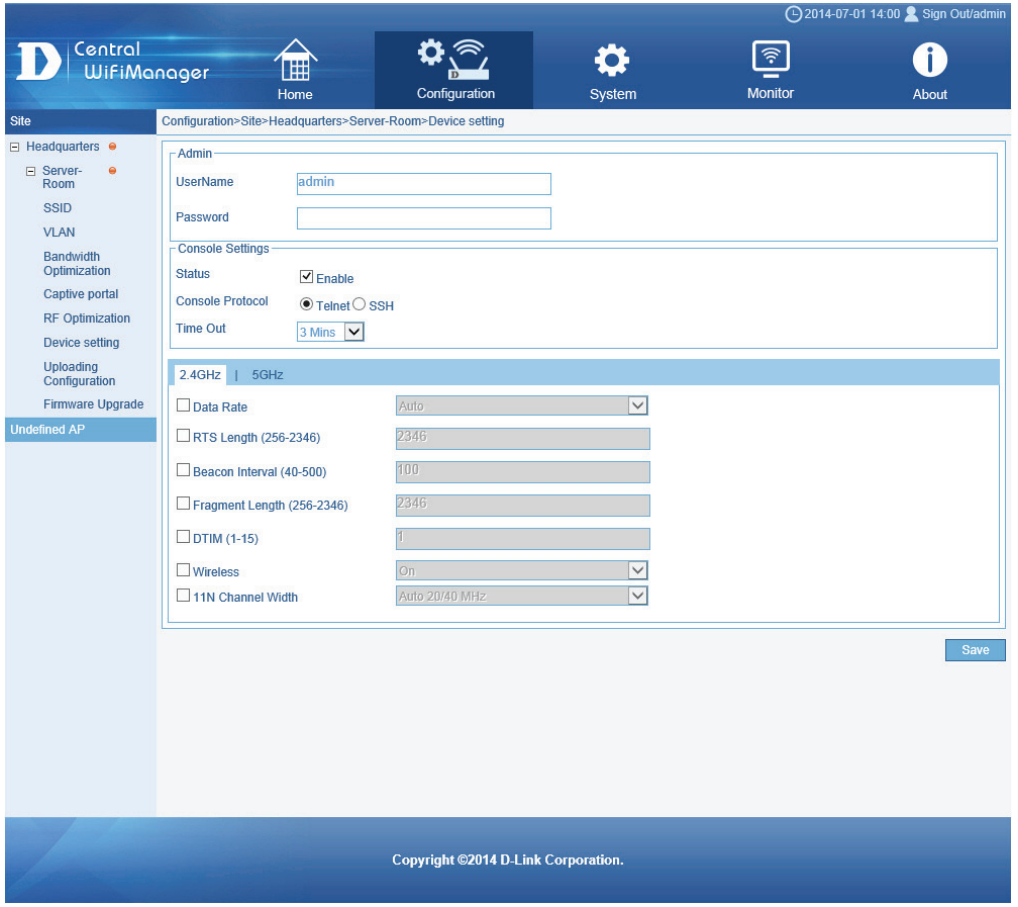
CWM Configuration | Configuration | Site | Network | **Device Settings**

After clicking on **Device Settings** in the left panel, the following page will be available. On this page we can view and configure the login and accessibility settings for access points in this network. Additionally some advanced wireless settings can be configured on this page for both the 2.4Ghz and 5Ghz frequency bands.

The following parameters can be configured.

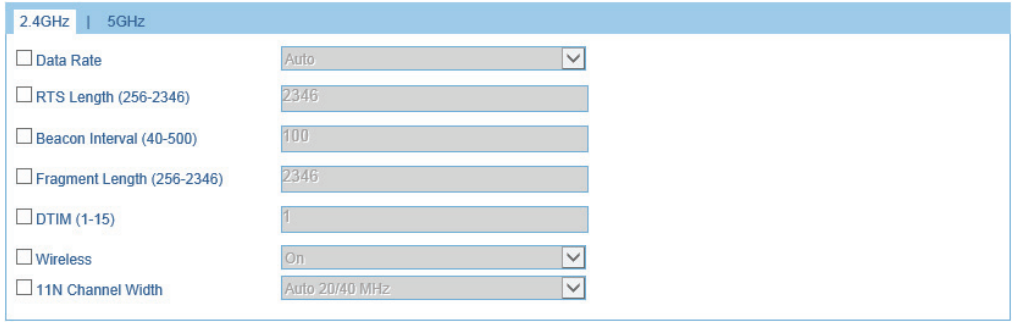
Parameter	Description
Username	This field displays the username that is applied to all access points in this network.
Password	Enter the password that will be applied to all access points in this network here.
Status	Select this option to enable console port connectivity on all access points in the network.
Console Protocol	Select the console port protocol that will be used on all access points in this network. Options to choose from are **Telnet** and **SSH**.
Time Out	Select the active console session time out value here. Options to choose from are **1 Min**, **3 Mins**, **5 Mins**, **10 Mins**, **15 Mins**, and **Never**.

Click the **Save** button to accept the changes made.



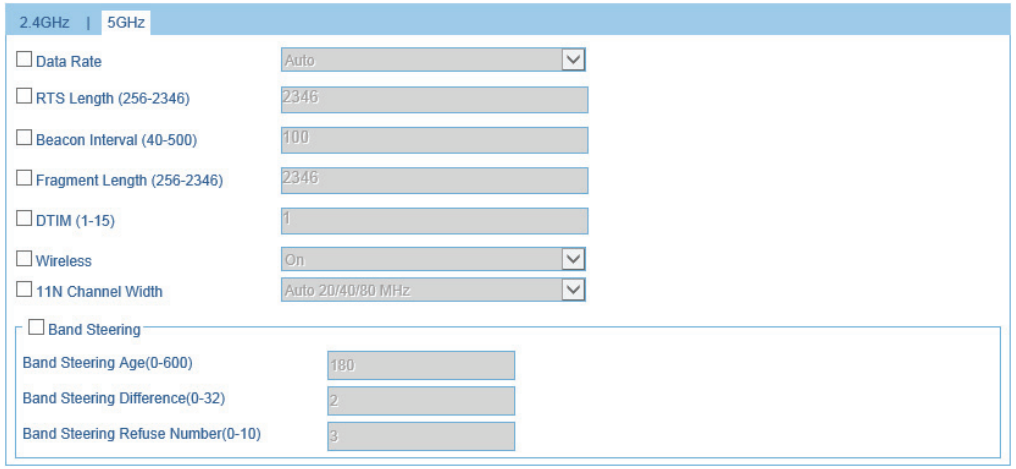
In the **2.4GHz** and **5GHz** sections the following parameters can be configured.

Parameter	Description
Data Rate	Select the wireless data rate that will be given the highest priority here. This rate is between 1 and 54 Mbps. Select **Auto** to allow the access point to determine the best rate.
RTS Length	Enter the RTS length value here. This value must be between 256 and 2346. By default, this value is 2346.
Beacon Interval	Enter the beacon interval value here. This value must be between 40 and 500. By default, this value is 100.
Fragment Length	Enter the fragment length value here. This value must be between 256 and 2346. By default, this value is 2346.
DTIM	Enter the DTIM value here. This value must be between 1 and 15. By default, this value is 1.
Wireless	Select whether the wireless connectivity of access points in this network should be **On** or **Off**.
11N Channel Width	Select the 802.11n wireless channel width here. Options to choose from are **20 MHz** and **Auto 20/40 MHz**. In the **5GHz** section, an additional **Auto 20/40/80 MHz** option is available for selection.



In the **5GHz** section the following additional parameters can be configured.

Parameter	Description
Band Steering Age	Enter the band steering age value here. This value must be between 0 and 600. By default, this value is 180.
Band Steering Difference	Enter the band steering difference value here. This value must be between 0 and 32. By default, this value is 2.
Band Steering Refuse Number.	Enter the band steering refuse number here. This value must be between 0 and 10. By default, this value is 3.

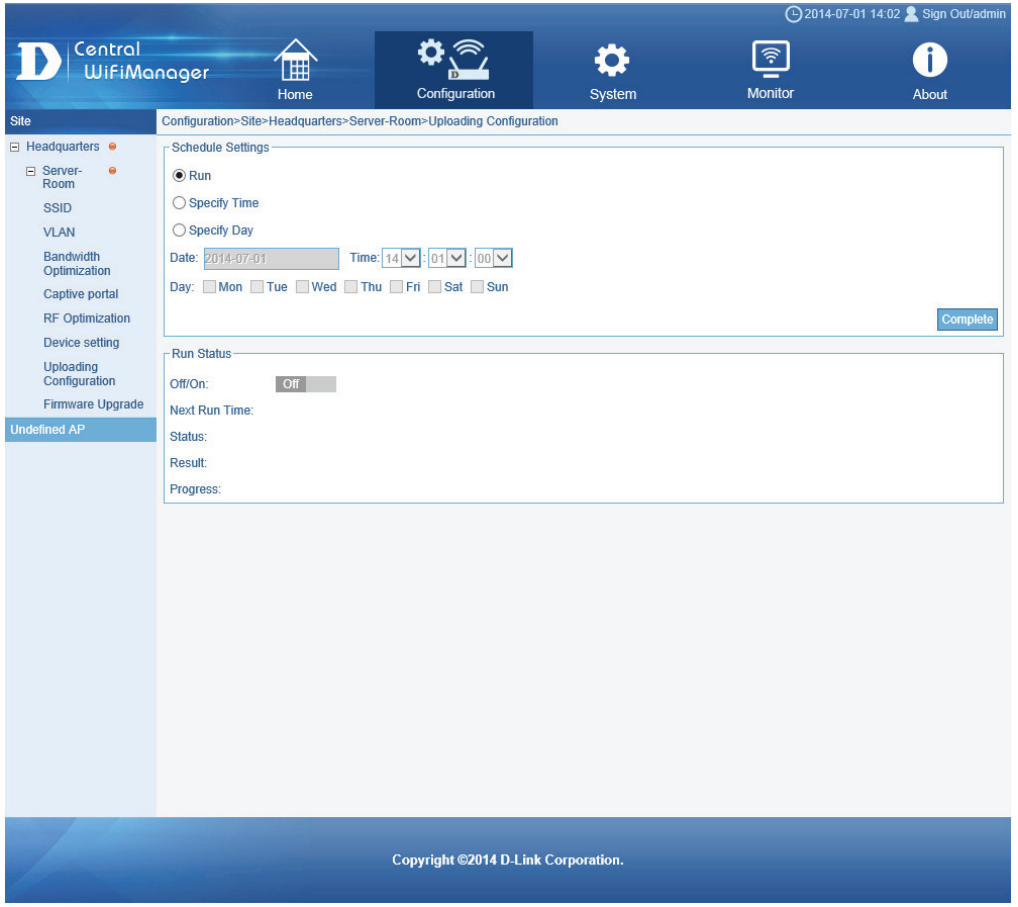


CWM Configuration | Configuration | Site | Network | **Upload Configuration**

After clicking on **Uploading Configuration** in the left panel, the following page will be available. On this page we can view and configure the configuration file upload schedule or initiate the upload of the configuration file to all access points in this network manually.

In the **Schedule Settings** section, the following parameters can be configured.

Parameter	Description
Run	Select this option to manually upload the configuration file to all the access points in this network manually. Click **Complete** to initiate the upload.
Specify Time	Select this option to configure the scheduled time for the configuration upload to take place. Selecting this option will initiate the configuration upload every weekday specified at the time specified continuously.
Specify Date	Select this option to configure the scheduled date for the configuration upload to take place. Selecting this option will only initiate the configuration upload once on the date and time specified.
Date	After selecting the **Specify Date** option, select the date at which the upload will be initiated.
Time	After selecting the **Specify Time** or the **Specify Date** option, select the time at which the upload will be initiated.
Day	After selecting the **Specify Time** option, select the day(s) on which the upload will be initiated.



Click the **Complete** button to accept the changes made or to manually initiate the upload.

In the **Run Status** section, the following parameters can be configured.

Parameter	Description
Off/On	Toggle this option to **On**, to enable the scheduled configuration upload configured. Toggle this option to **Off** to disable the scheduled upload. To reconfigure the schedule settings, this option must be turned off.

After the first upload, the **Next Run Time** field will display when the next upload will take place. After every upload, the **Result** hyperlink will be made available for review.

CWM Configuration | Configuration | Site | Network | **Firmware Upgrade**

After clicking on **Firmware Upgrade** in the left panel, the following page will be available. On this page we can view and configure the firmware file upload schedule or initiate the upload of the firmware file to all access points in this network manually.

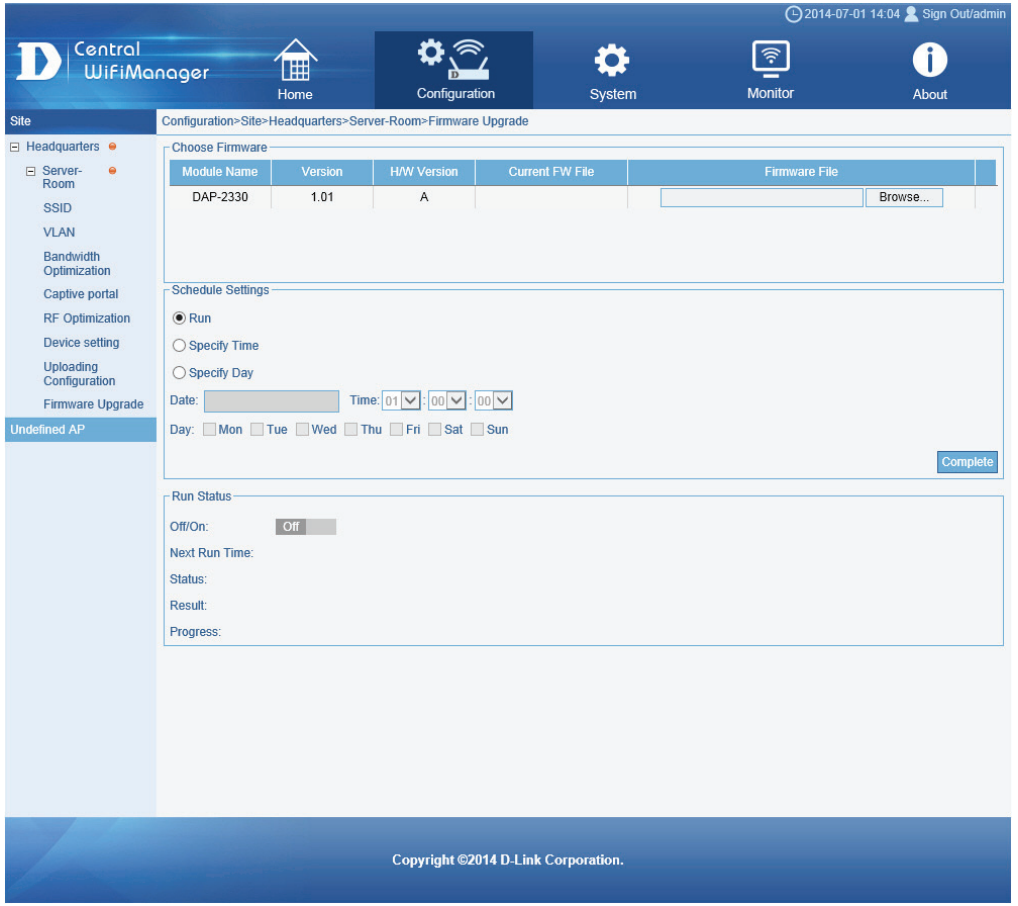
In the **Choose Firmware** section, the following parameters can be configured.

Parameter	Description
Firmware File	For every access point in this network, we can specify the firmware file that will be uploaded either manually, or based on the schedule configured. Click **Browse** to navigate to the firmware file located on the computer.

In the **Schedule Settings** section, the following parameters can be configured.

Parameter	Description
Run	Select this option to manually upload the firmware file to all the specified access points in this network manually. Click **Complete** to initiate the upload.
Specify Time	Select this option to configure the scheduled time for the firmware upload to take place. Selecting this option will initiate the firmware upload every weekday specified at the time specified continuously.
Specify Date	Select this option to configure the scheduled date for the firmware upload to take place. Selecting this option will only initiate the firmware upload once on the date and time specified.
Date	After selecting the **Specify Date** option, select the date at which the upload will be initiated.
Time	After selecting the **Specify Time** or the **Specify Date** option, select the time at which the upload will be initiated.
Day	After selecting the **Specify Time** option, select the day(s) on which the upload will be initiated.

Click the **Complete** button to accept the changes made or to manually initiate the upload.

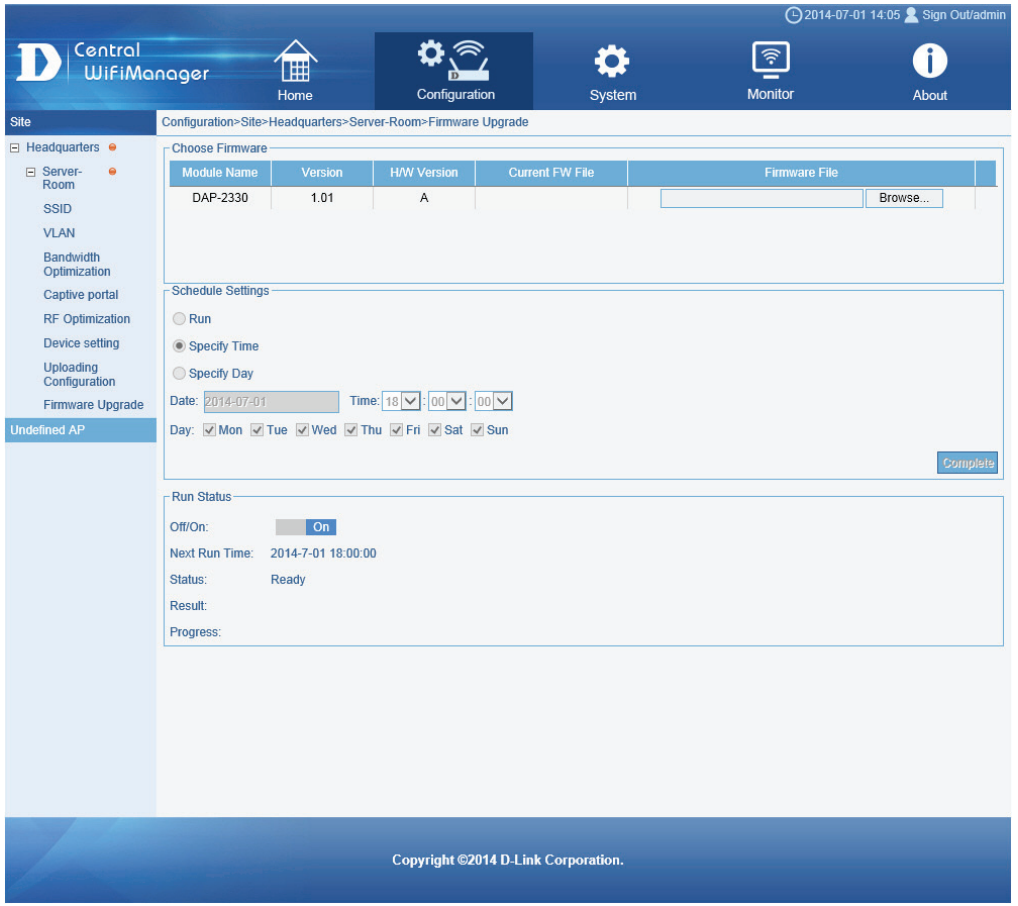


CWM Configuration | Configuration | Site | Network | **Firmware Upgrade**

In the **Run Status** section, the following parameters can be configured.

Parameter	Description
Off/On	Toggle this option to **On**, to enable the scheduled firmware upload configured. Toggle this option to **Off** to disable the scheduled upload. To reconfigure the schedule settings, this option must be turned off.

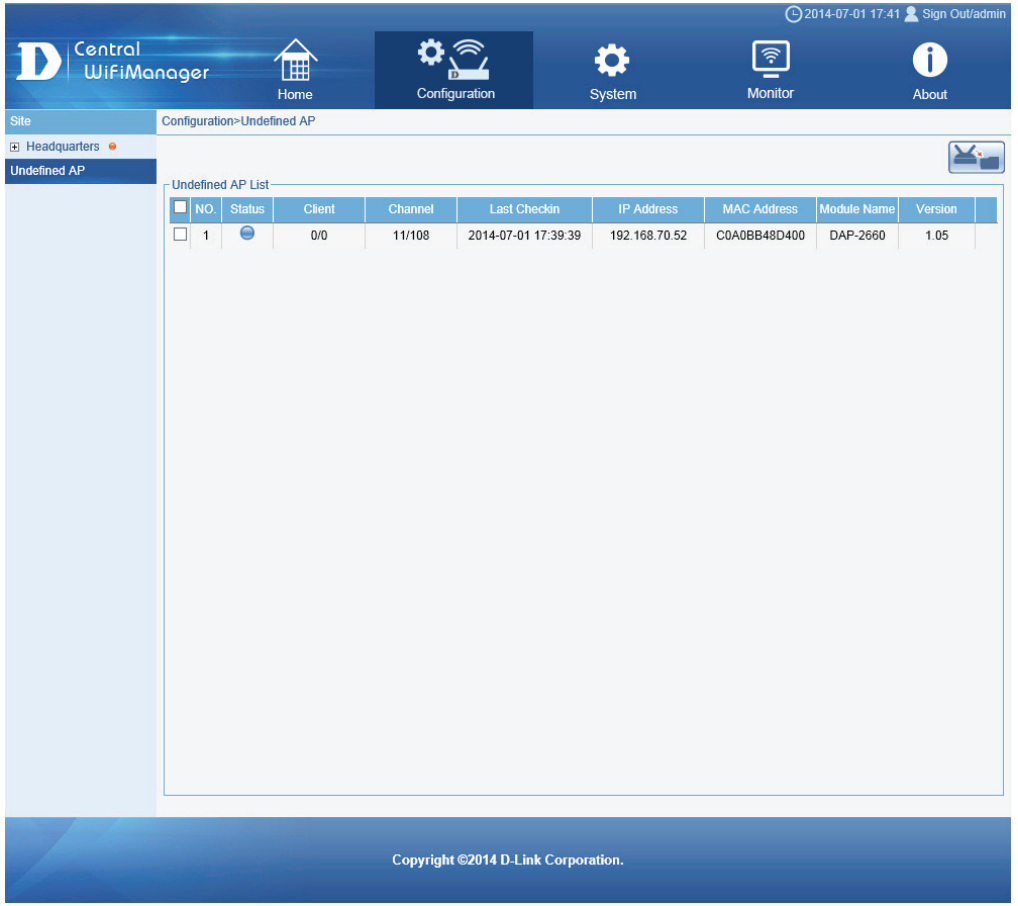
After the first upload, the **Next Run Time** field will display when the next upload will take place. After every upload, the **Result** hyperlink will be made available for review.



CWM Configuration Configuration Undefined AP

After clicking on **Undefined AP** in the left panel, the following page will be available. On this page we can view a list of access points that do not belong to a network configured in any site.

To add an access point in this list to a network, select the check box next to the entry and click the icon on the top, right of this page. A list of available networks will be displayed that can be selected for the move.



CWM Configuration | System | Settings | General

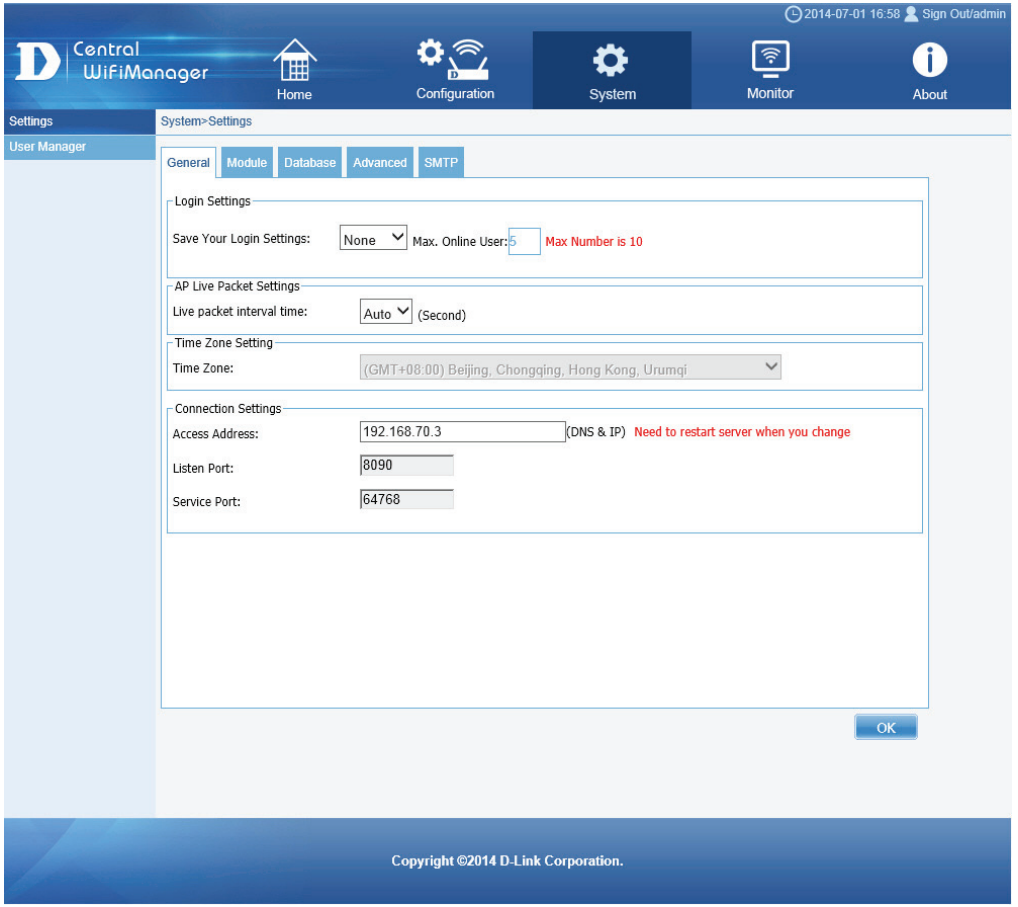
On this page we can view and configure settings that are related to the system functionality of the Central WifiManager application.

In the following sections we will discuss these settings in more detail.

After clicking on **System** in the top panel and **Settings** in the left panel, the following page will be displayed. On this page there are five tabs with various settings that can be configured. They are **General**, **Module**, **Database**, **Advance** and **SMTP**.

In the **General** tab, the following parameters can be configured.

Parameter	Description
Save Your Login Settings	In the **Login Settings** section, select this option to choose whether the login session should be remembered or not. After selecting the **None** option, the user will be prompt to login every time a connection to the Web User Interface (Web UI) is made. After selecting the **1 week** option, the user session will be kept open for one week. During this time, the user will not be asked to login again after the initial login was made except if the user manually logged out.
Max. Online User	In the **Login Settings** section, enter the maximum amount of users that will be allowed to access the management interface at the same time. This value must be between 1 and 10. By default, this value is 5.
Live packet interval time	In the **AP List Packet Settings** section, select the live packet interval time here. Options to choose from are **Auto**, **2**, **5**, **10**, **20**, and **30**.
Time Zone	In the **Time Zone Settings** section, select the correct time zone option here.
Access Address	In the **Connection Settings** section, enter the Central WifiManager Server application's IP address here.
Listen Port	In the **Connection Settings** section, enter the Central WifiManager Server application's listen port number here. By default, this value is 8090.
Service Port	In the **Connection Settings** section, enter the Central WifiManager Server application's service port number here. By default, this value is 64768.

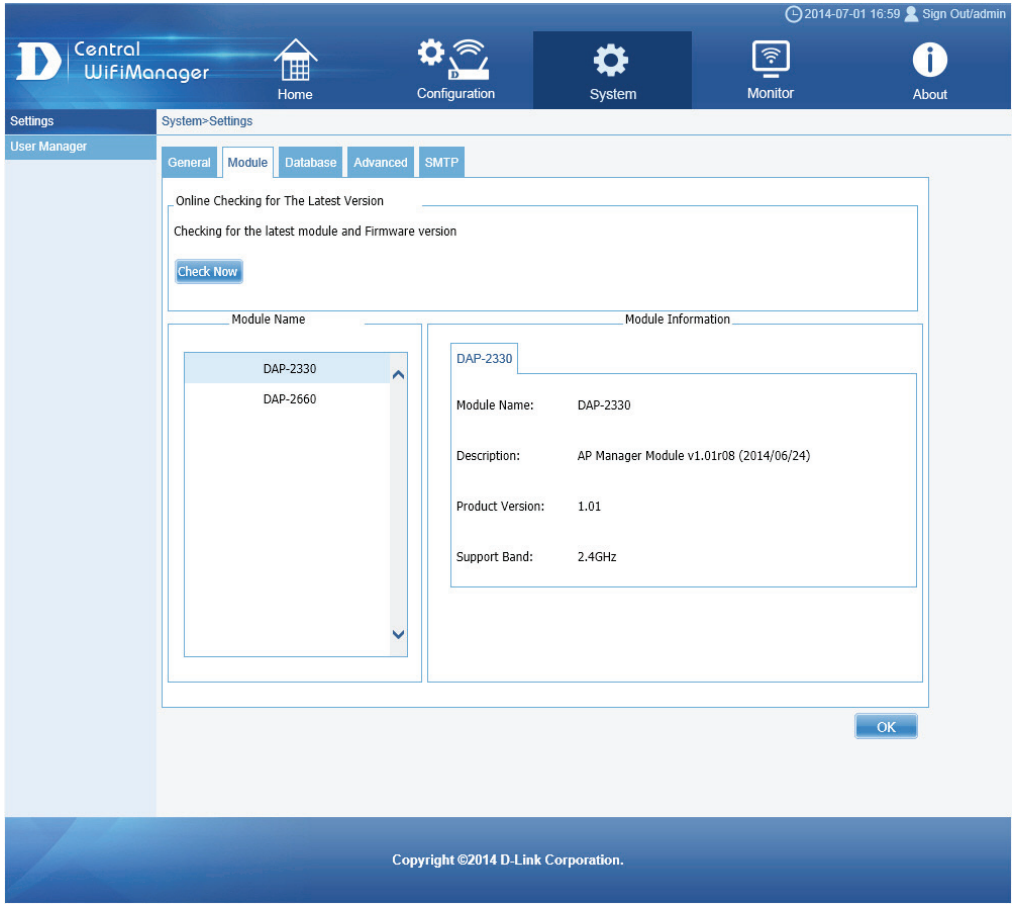


Click the **OK** button to accept the changes made.

CWM Configuration | System | Settings | Module

In the **Module** tab, a list of access point modules will be displayed in the **Module Name** section. Every different model of access point that will be managed by the Central WifiManager Server application, requires the administrator to install the executable module file for that specific access point's model name.

For example, on this page we have two kinds of access point modules installed, the DAP-2330 and the DAP-2660. This means that we can have multiple DAP-2330 and DAP-2660 access points installed on the network, but only required to install two modules. One for each type of access point.

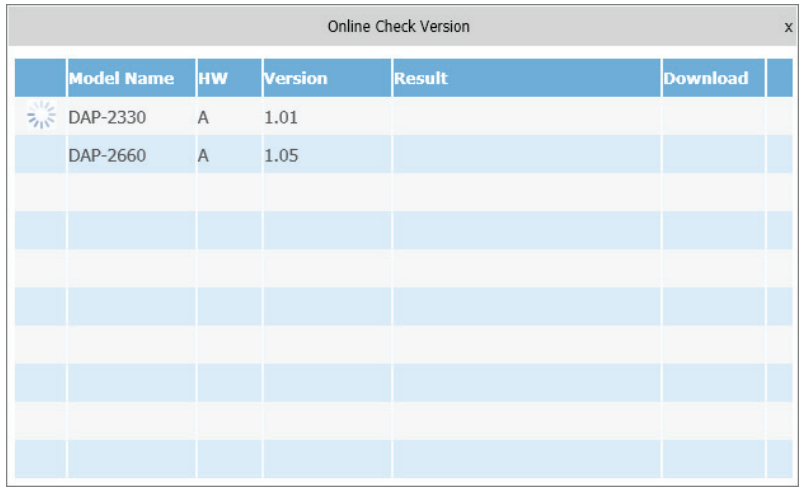


NOTE: The module executable files for all the access points, supported in the application, can be downloaded from the D-Link website.

More information about the installed access point modules can be found in the **Module Information** section.

To keep the installed modules and firmware versions for access points up to date, click on the **Check Now** button.

Click the **OK** button to accept the changes made.



After clicking on **Check Now**, the following page will be available. On this page the application will check if the installed access point modules are up to date.

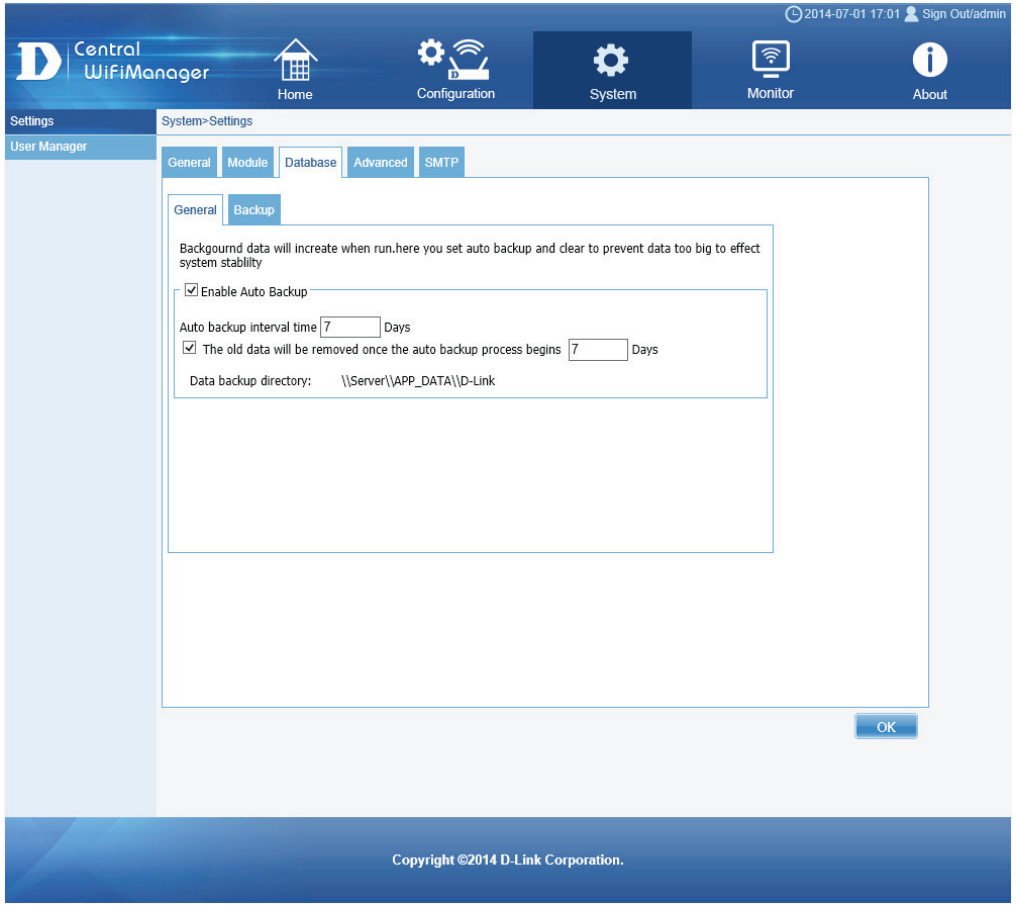
CWM Configuration | System | Settings | Database

After clicking on the **Database** tab, the following page will be available. On this page we can view and configure how this application backs up or restores the database information and at what time intervals this should take place. In the **Database** tab, there are two sub-tab pages called **General** and **Backup**.

In the **General** sub-tab, the following parameters can be configured.

Parameter	Description
Enable Auto Backup	Select this option to enable the automatic backup feature of the application's database.
Auto backup interval time	Enter the automatic backup interval time, in days, here. By default, this value is 7 days. To remove the old database backed up information after the new database was successfully backed up, select the '**The old data will be removed once the auto backup process begins**' option and enter the pending days value in the text box. By default, this value is 7 days.
Data backup directory	In this field the path to the backup directory will be displayed for reference.

Click the **OK** button to accept the changes made.

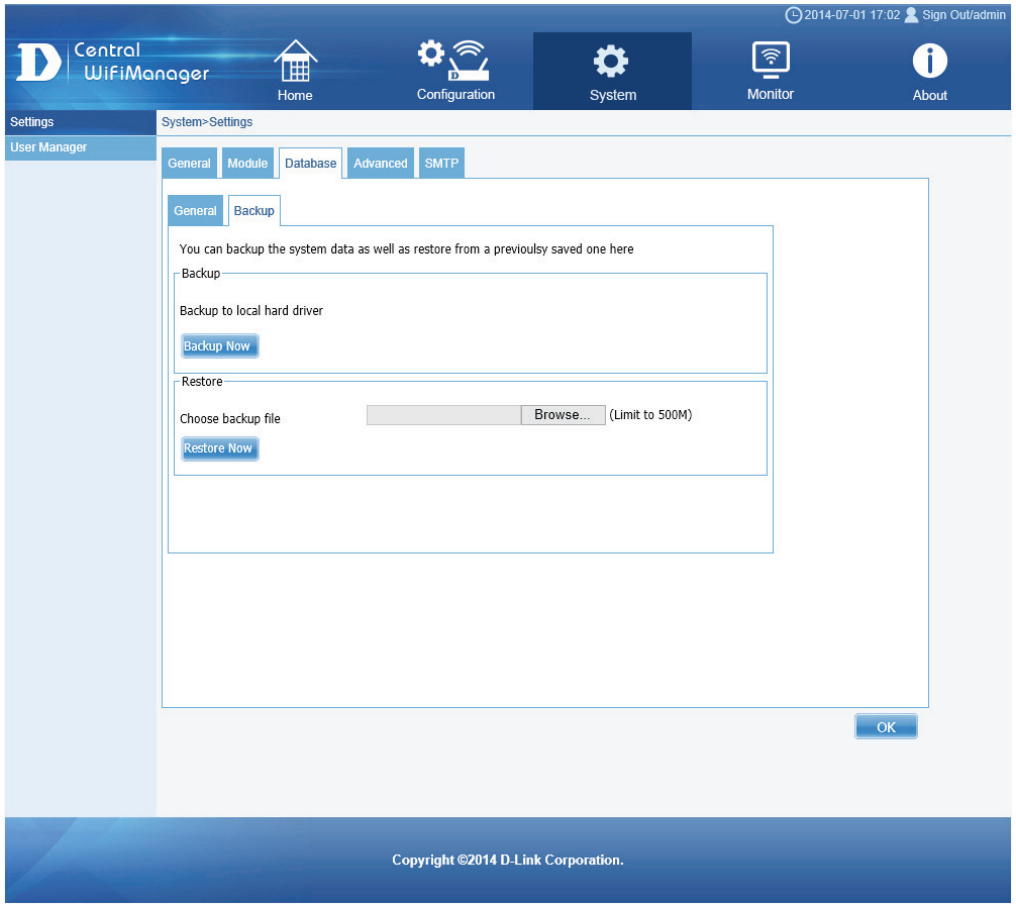


CWM Configuration | System | Settings | Database

In the **General** sub-tab, the following parameters can be configured.

Parameter	Description
Backup	In this section we can manually backup the system data to the computer accessing the Web interface. Click **Backup Now** to initiate the manual backup. The backup file is a PostgreSQL file with the file extension of SQL.
Restore	In this section we can manually navigate to a backed up file and restore those settings to this application. Click **Browse** and navigate to the previously backed up SQL file and then click **Restore Now** to initiate the restore.

Click the **OK** button to accept the changes made.



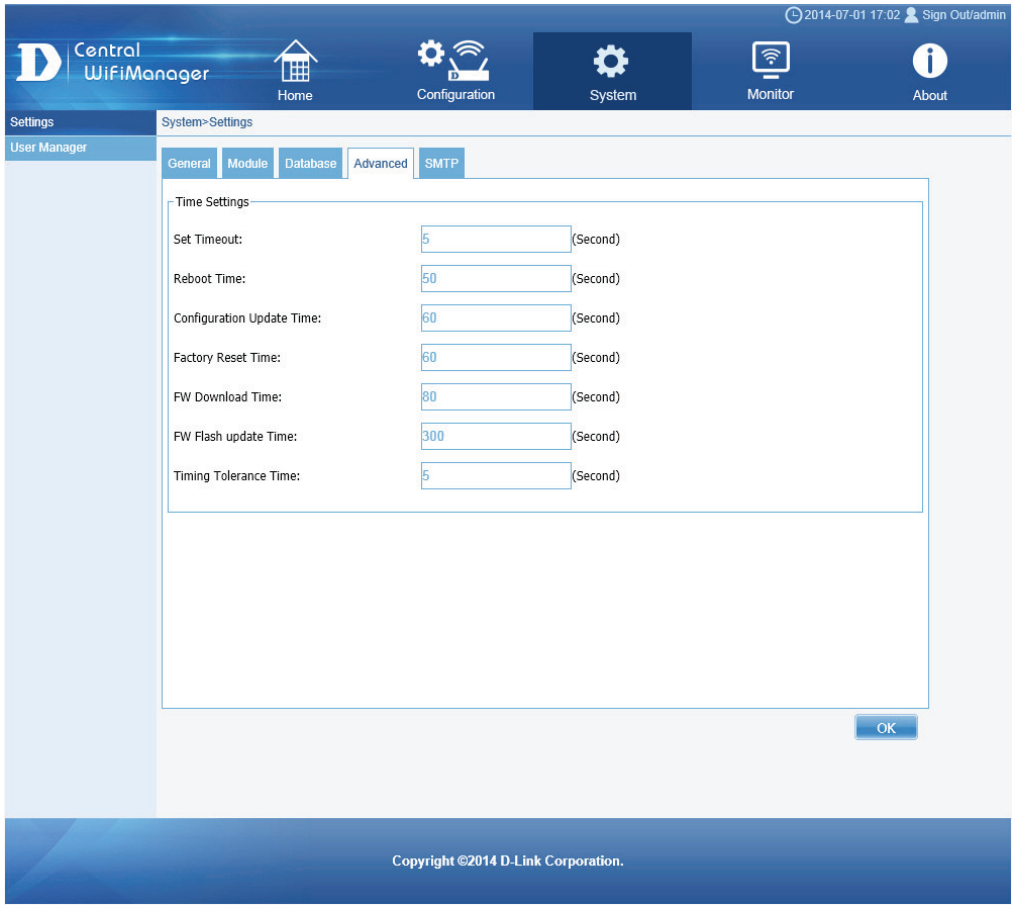
CWM Configuration | System | Settings | Advanced

After clicking on the **Advanced** tab, the following page will be available. On this page we can view and configure advanced time settings for some features hosted by this application.

The following parameters can be configured.

Parameter	Description
Set Timeout	Enter the maximum time allowed for settings to be made in this application. This is the time from the click of a button until the request was received by the server. By default, this value is 5 seconds.
Reboot Time	Enter the time the Web application will wait after a reboot request was send by the server to access points. By default, this value is 50 seconds.
Configuration Update Time	Enter the time the Web application will wait after a configuration file update was initiated to access points by the server. By default, this value is 60 seconds.
Factory Reset Time	Enter the time the Web application will wait after a factory reset was initiated to access points by the server. By default, this value is 60 seconds.
FW Download Time	Enter the time the Web application will allow for firmware downloads initiated by the firmware update check feature. By default, this value is 80 seconds.
FW Flash Update Time	Enter the time the Web application will wait after a firmware flash update was initiated by the server to access points. By default, this value is 300 seconds.
Timing Tolerance Time	Enter the timing tolerance time value here. By default, this value is 5 seconds.

Click the **OK** button to accept the changes made.

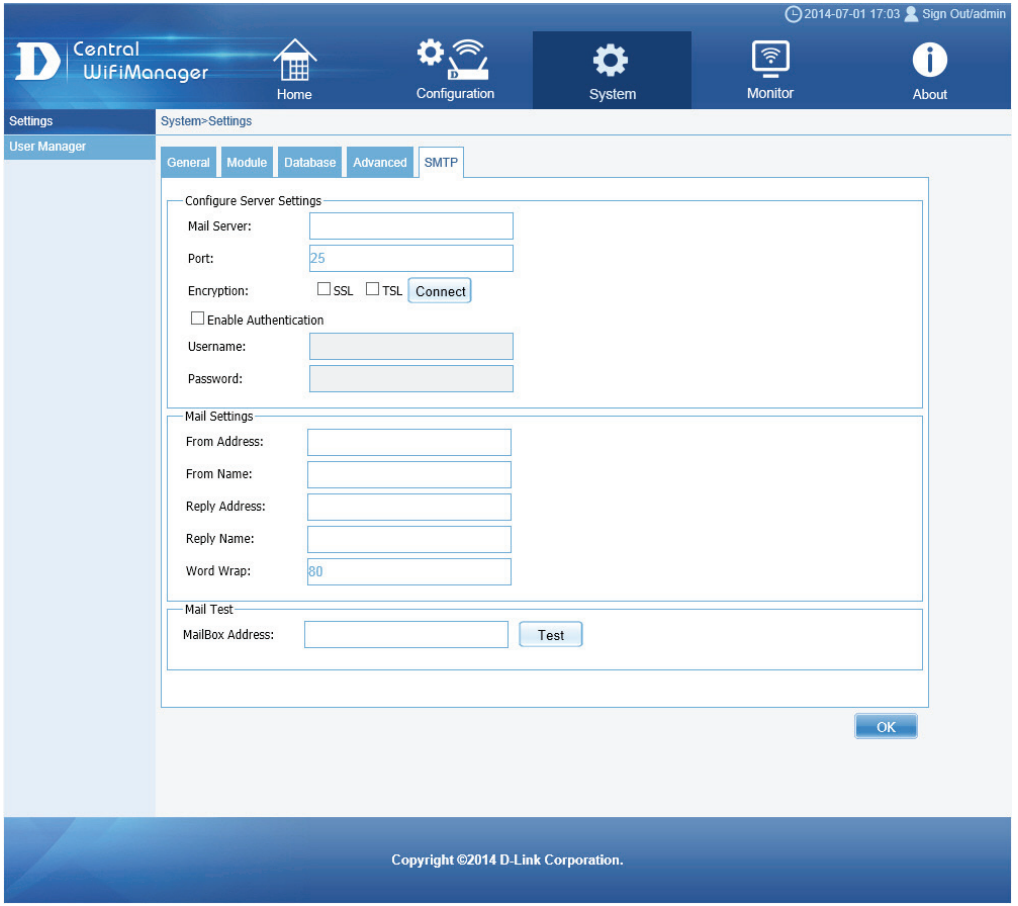


CWM Configuration | System | Settings | SMTP

After clicking on the **SMTP** tab, the following page will be available. On this page we can view and configure the Simple Mail Transfer Protocol (SMTP) settings.

In the **Configure Server Settings** section, the following parameters can be configured.

Parameter	Description
Mail Server	Enter the SMTP server's IP address or domain name here.
Port	Enter the SMTP server's port number here. By default, this value is 25.
Encryption	If applicable, select the SMTP connection's encryption method here. Options available are **SSL** and **TSL**. Click **Connect** to test if the mail server settings are correct.
Enable Authentication	Select this option if the SMTP server requires authentication to successfully send emails.
Username	After authentication was enabled, enter the SMTP user account's username here.
Password	After authentication was enabled, enter the SMTP user account's password here.



In the **Mail Settings** section, the following parameters can be configured.

Parameter	Description
From Address	Enter the sender's email address here so that the recipient can recognize who is sending the email.
From Name	Enter the sender's name here.
Reply Address	Enter the recipient's email address here.
Reply Name	Enter the recipient's name here.
Word Wrap	Enter the word wrap value here. By default, this value is 80.

In the **Mail Test** section, the following parameters can be configured.

Parameter	Description
Mailbox Address	To test if the recipient's email address is active, enter the recipient's email address here and click **Test**.

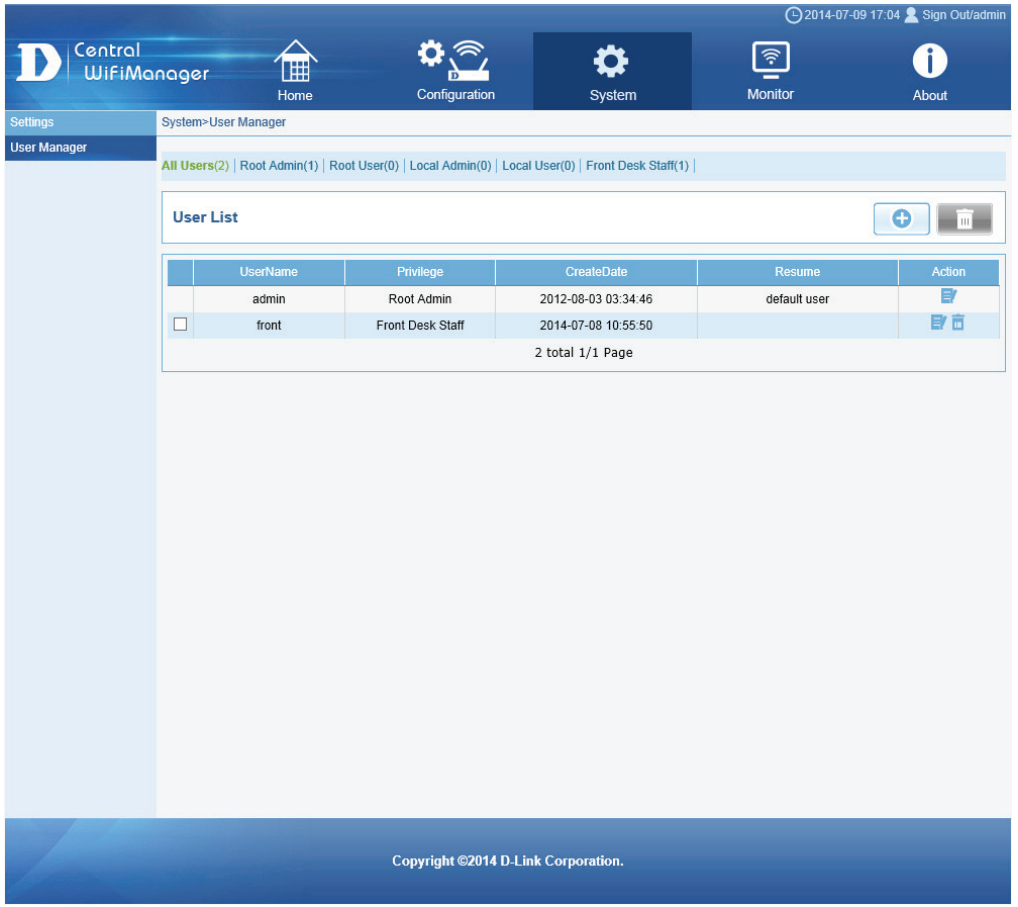
Click the **OK** button to accept the changes made.

CWM Configuration System User Manager

After clicking on **System** in the top panel and **User Manager** in the left panel, the following page will be displayed. On this page we can view, create and configure user accounts. There are five kinds of user accounts that can be created to access the Central WifiManager Server application.

In the **User List** section, a list of user accounts will be displayed.

Click the button to add a new user account.
Click the icon to modify an existing user account.
Click the icon to delete an existing user account.

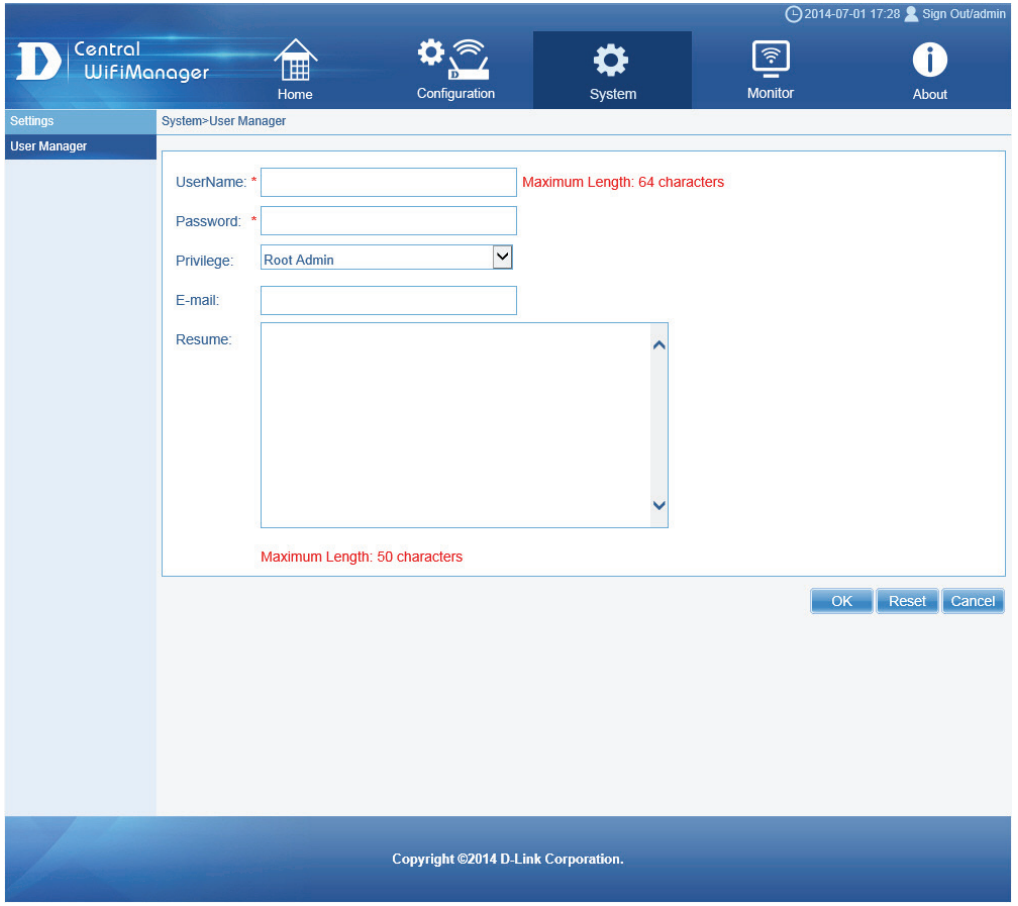


CWM Configuration | System | User Manager | Create User Account

After clicking the icon, the following page will be available. On this page we can configure the following parameters.

Parameter	Description
Username	Enter the username for the new user account here. This name must be between 4 and 64 characters long.
Password	Enter the password for the new user account here. This password must be between 4 and 64 characters long.
Privilege	Select the privilege level that this user account will have. Options to choose from are **Root Admin**, **Root User**, **Local Admin**, **Local User**, and **Front Desk Staff**.
E-mail	Enter the email address that will be associated with this user account here.
Resume	Enter a more detailed description for this user account here.

Click the **OK** button to create the user account.
Click the **Reset** button to clear the information entered in the fields of this form.
Click the **Cancel** button to discard the changes made and return to the main page.



CWM Configuration | Monitor | Report | Association | **By Access Point**

After clicking on **Monitor** in the top panel and **Association** in the left panel, the following page will be displayed. On this page we can view a report of all the access points and wireless clients managed by this application. Three association reports can be generated **By Access Point**, **By Wireless Station**, and **By Station Number**.

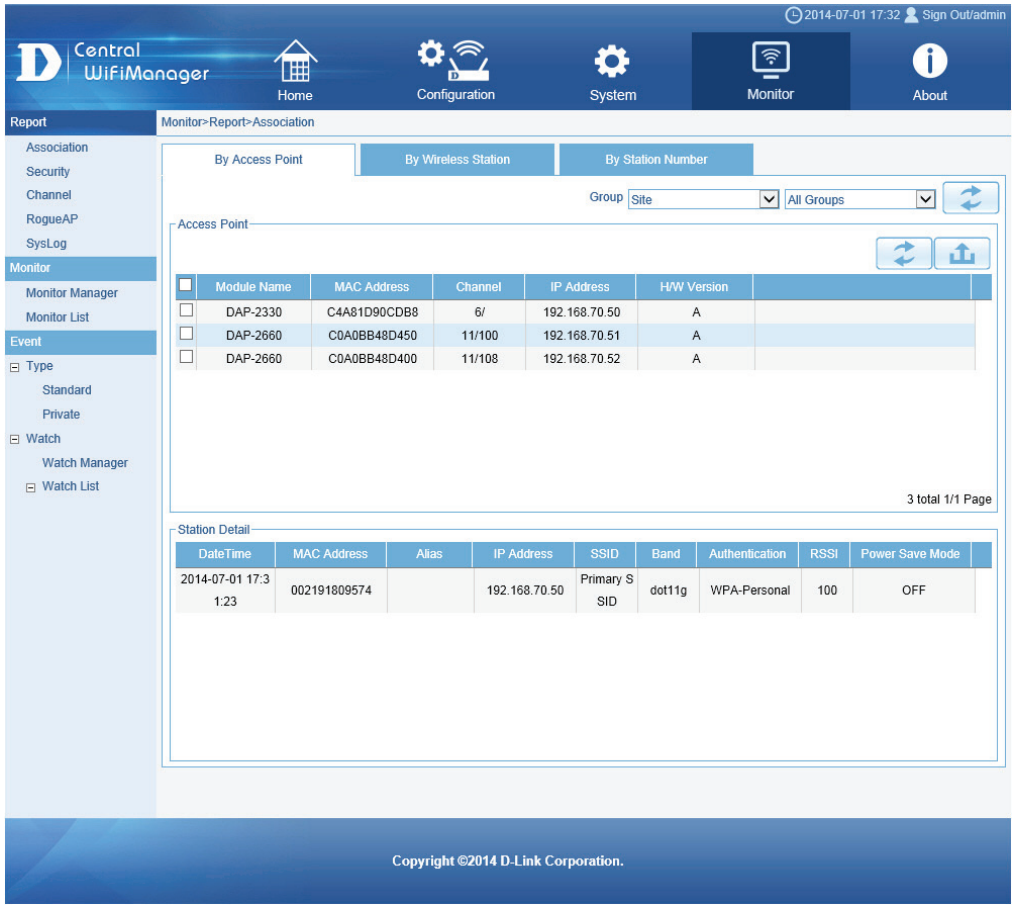
On this page a report was generated **By Access Point**. This report can be refined by selecting the **Group** (Site), from the first drop-down menu, and also then selecting the network in the second drop-down menu.

Click the button to regenerate this report.

In the **Access Point** table the list of access points, managed by this application, will be displayed. Information like the **Module Name**, **MAC Address**, **Channel**, **IP Address** and **HW Version** is displayed for each access point.

In the **Station Detail** table the list of wireless clients, connected to the access points, managed by this application, will be displayed. Information like **Date/Time**, **MAC Address**, **Alias**, **IP Address**, **SSID**, **Band**, **Authentication**, **RSSI** and **Power Save Mode** is displayed for each wireless client.

Click the button to export the contents displayed in these tables to the computer accessing this interface. This export supports the following file formats; **TXT**, **PDF** and **Excel**.



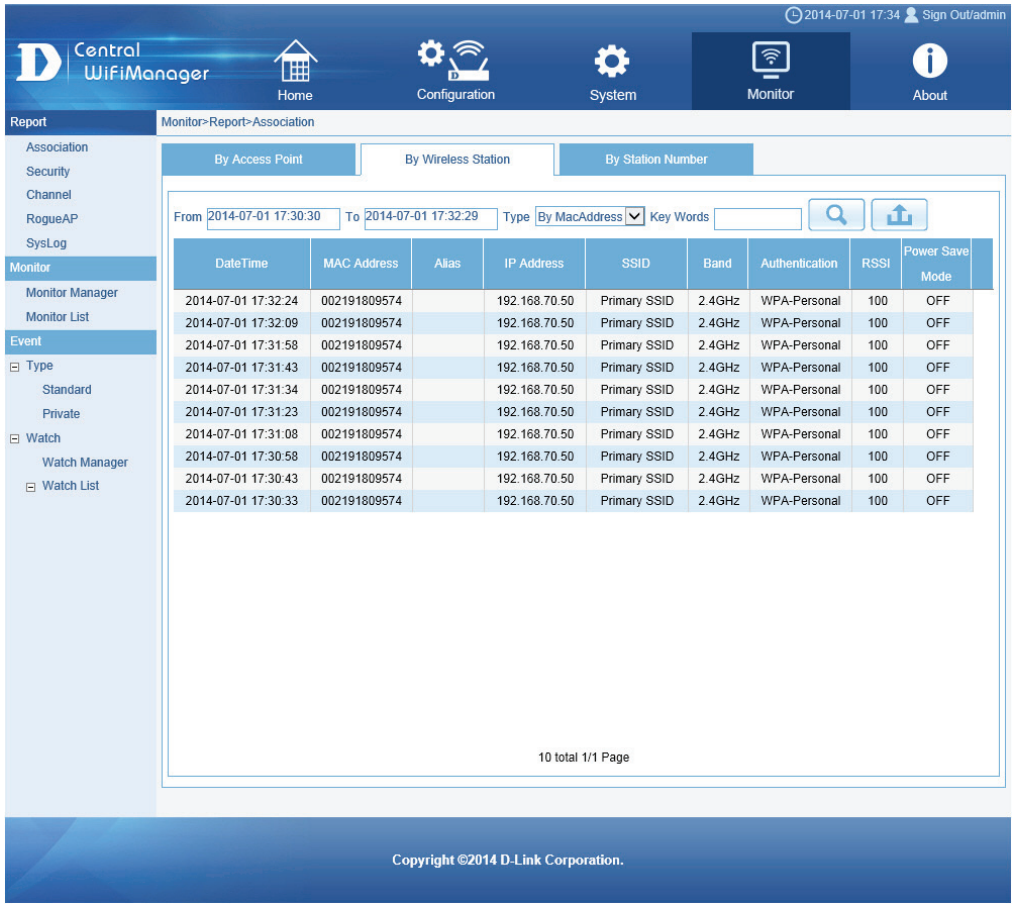
CWM Configuration | Monitor | Report | Association | **By Wireless Station**

On this page a report was generated **By Wireless Station**. This report can be refined by selecting the date and time **From** and **To**, and then selecting the **Type**, either **By MAC Address** or **By Alias**, and also additionally entering **Key Words** in the text box provided.

Click the button to regenerate this report.

In the table a list of wireless client connections, connected to the access points, managed by this application, will be displayed. Information like **Date/Time**, **MAC Address**, **Alias**, **IP Address**, **SSID**, **Band**, **Authentication**, **RSSI** and **Power Save Mode** is displayed for each wireless client.

Click the button to export the contents displayed in this table to the computer accessing this interface. This export supports the following file formats; **TXT**, **PDF** and **Excel**.


2014-07-01 17:34 Sign Out/admin
Central WifiManager
Home
Configuration
System
Monitor
About
Report
Association
Security
Channel
RogueAP
SysLog
Monitor
Monitor Manager
Monitor List
Event
Type
Standard
Private
Watch
Watch Manager
Watch List
Monitor>Report>Association
By Access Point
By Wireless Station
By Station Number
From 2014-07-01 17:30:30 To 2014-07-01 17:32:29 Type By MacAddress Key Words
DateTime | MAC Address | Alias | IP Address | SSID | Band | Authentication | RSSI | Power Save Mode
2014-07-01 17:32:24 | 002191809574 | | 192.168.70.50 | Primary SSID | 2.4GHz | WPA-Personal | 100 | OFF
2014-07-01 17:32:09 | 002191809574 | | 192.168.70.50 | Primary SSID | 2.4GHz | WPA-Personal | 100 | OFF
2014-07-01 17:31:58 | 002191809574 | | 192.168.70.50 | Primary SSID | 2.4GHz | WPA-Personal | 100 | OFF
2014-07-01 17:31:43 | 002191809574 | | 192.168.70.50 | Primary SSID | 2.4GHz | WPA-Personal | 100 | OFF
2014-07-01 17:31:34 | 002191809574 | | 192.168.70.50 | Primary SSID | 2.4GHz | WPA-Personal | 100 | OFF
2014-07-01 17:31:23 | 002191809574 | | 192.168.70.50 | Primary SSID | 2.4GHz | WPA-Personal | 100 | OFF
2014-07-01 17:31:08 | 002191809574 | | 192.168.70.50 | Primary SSID | 2.4GHz | WPA-Personal | 100 | OFF
2014-07-01 17:30:58 | 002191809574 | | 192.168.70.50 | Primary SSID | 2.4GHz | WPA-Personal | 100 | OFF
2014-07-01 17:30:43 | 002191809574 | | 192.168.70.50 | Primary SSID | 2.4GHz | WPA-Personal | 100 | OFF
2014-07-01 17:30:33 | 002191809574 | | 192.168.70.50 | Primary SSID | 2.4GHz | WPA-Personal | 100 | OFF
10 total 1/1 Page
Copyright ©2014 D-Link Corporation.

CWM Configuration | Monitor | Report | Association | **By Station Number**

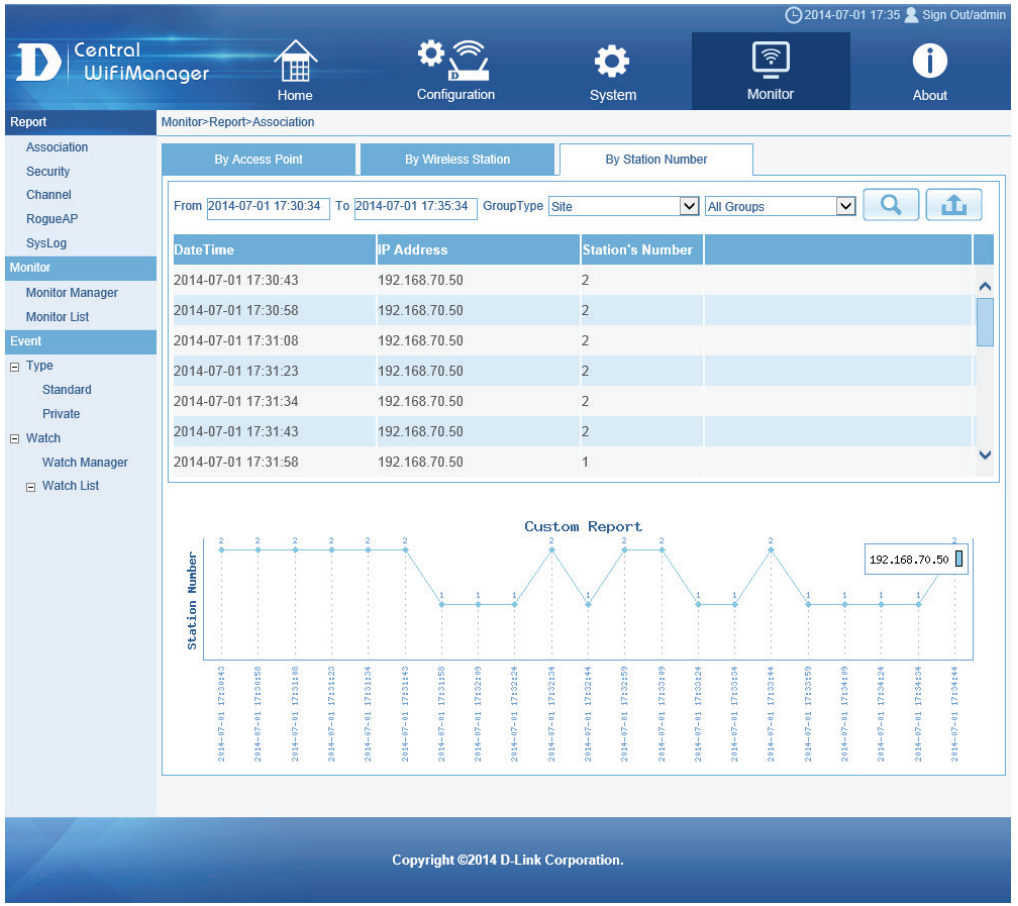
On this page a report was generated **By Station Number**. This report can be refined by selecting the date and time **From** and **To**, and then selecting the **Group Type** (Site), in the first drop-down menu, and then selecting the network in the second drop-down menu.

Click the button to regenerate this report.

In the table a list of access points will be displayed, by station number, if they have active wireless client connections, connected to the access points, managed by this application. Information like **Date/Time**, **IP Address** and **Station's Number** is displayed for each station.

In the line graph, a graphical representation of the **Station Number** over time will be displayed per IP address.

Click the button to export the contents displayed in this table and chart to the computer accessing this interface. This export supports the following file formats; **TXT**, **PDF** and **Excel**.



CWM Configuration | Monitor | Report | Security | **Chart**

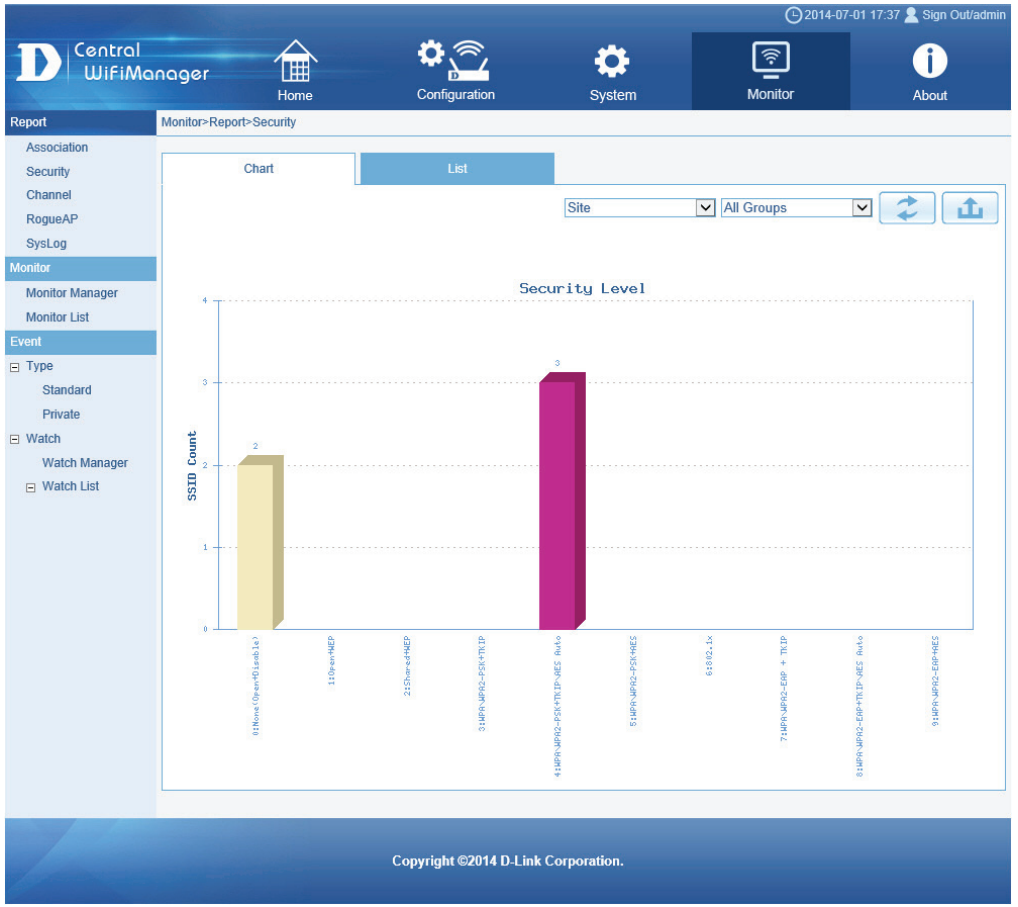
After clicking on **Monitor** in the top panel and **Security** in the left panel, the following page will be displayed. On this page we can view a report of the wireless security configurations of all the access points managed by this application. Security reports are displayed by **Chart** or by **List**.

On this page a **Chart** report was generated displaying all the available security levels on the access points managed by this application. This report can be refined by selecting the **Site**, in the first drop-down menu, and then selecting the network in the second drop-down menu.

Click the button to regenerate this report.

This report counts the available amount of SSIDs hosted by the access points in the network and then evaluating which security level they are configured at and then presenting them graphically in this chart per security level.

Click the button to export the contents displayed in this chart to the computer accessing this interface. This export supports the following file formats; **TXT**, **PDF** and **Excel**.



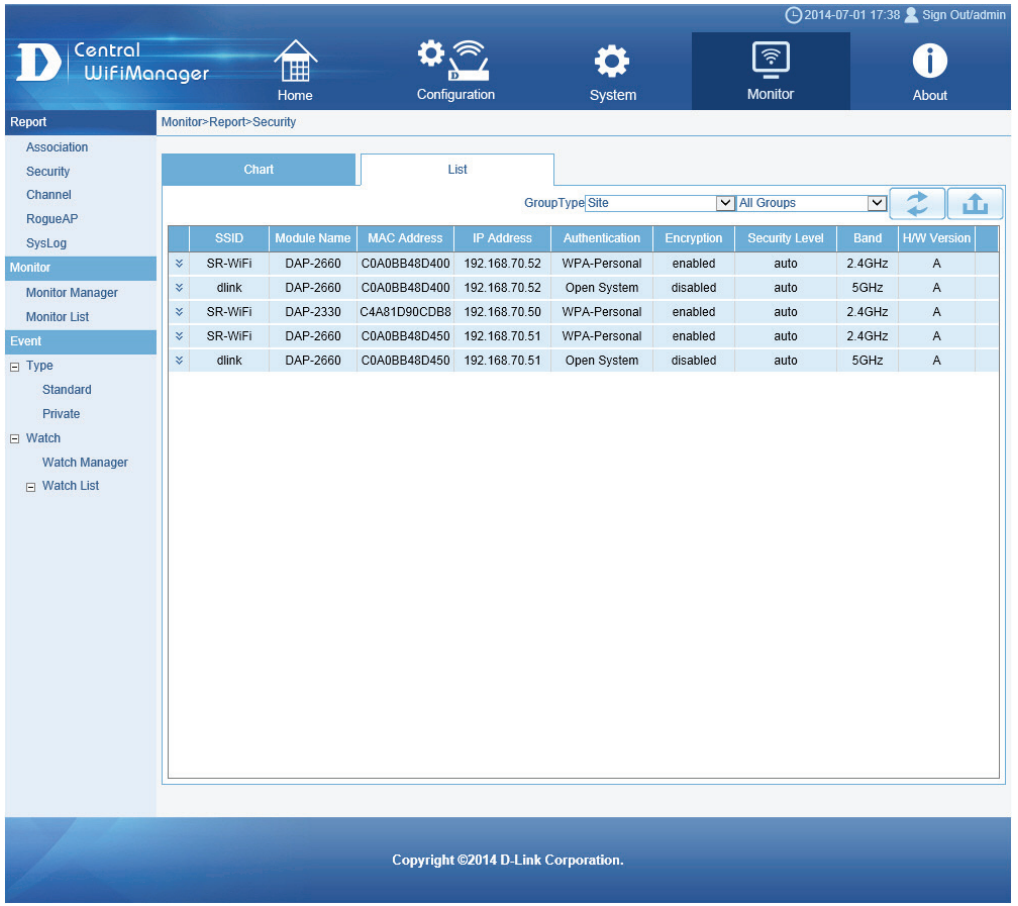
CWM Configuration | Monitor | Report | Security | List

On this page a **List** report was generated displaying all the SSIDs hosted by the access points managed by this application. This report can be refined by selecting the **Group Type** (Site), in the first drop-down menu, and then selecting the network in the second drop-down menu.

Click the button to regenerate this report.

Information like **SSID**, **Module Name**, **MAC Address**, **IP Address**, **Authentication**, **Encryption**, **Security Level**, **Band** and **HW Version** is displayed for each SSID.

Click the button to export the contents displayed in this table to the computer accessing this interface. This export supports the following file formats; **TXT**, **PDF** and **Excel**.



CWM Configuration | Monitor | Report | **Channel**

After clicking on **Monitor** in the top panel and **Channel** in the left panel, the following page will be displayed. On this page we can view a graphical chart report of the wireless channel usage per frequency band.

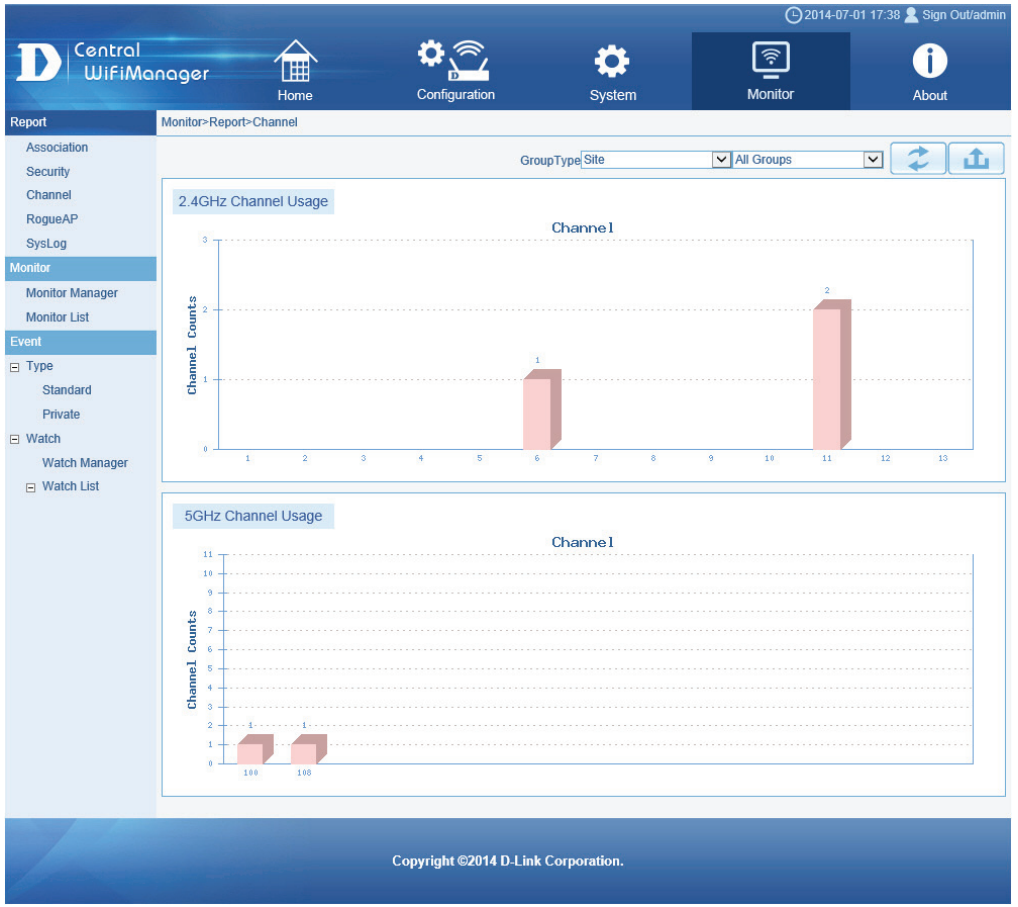
This report can be refined by selecting the **Group Type** (Site), in the first drop-down menu, and then selecting the network in the second drop-down menu.

Click the button to regenerate this report.

In the first chart report, we can view the channel number count for the 2.4GHz wireless frequency band.

In the second chart report, we can view the channel number count for the 5GHz wireless frequency band.

Click the button to export the contents displayed in these charts to the computer accessing this interface. This export supports the following file formats; **TXT**, **PDF** and **Excel**.



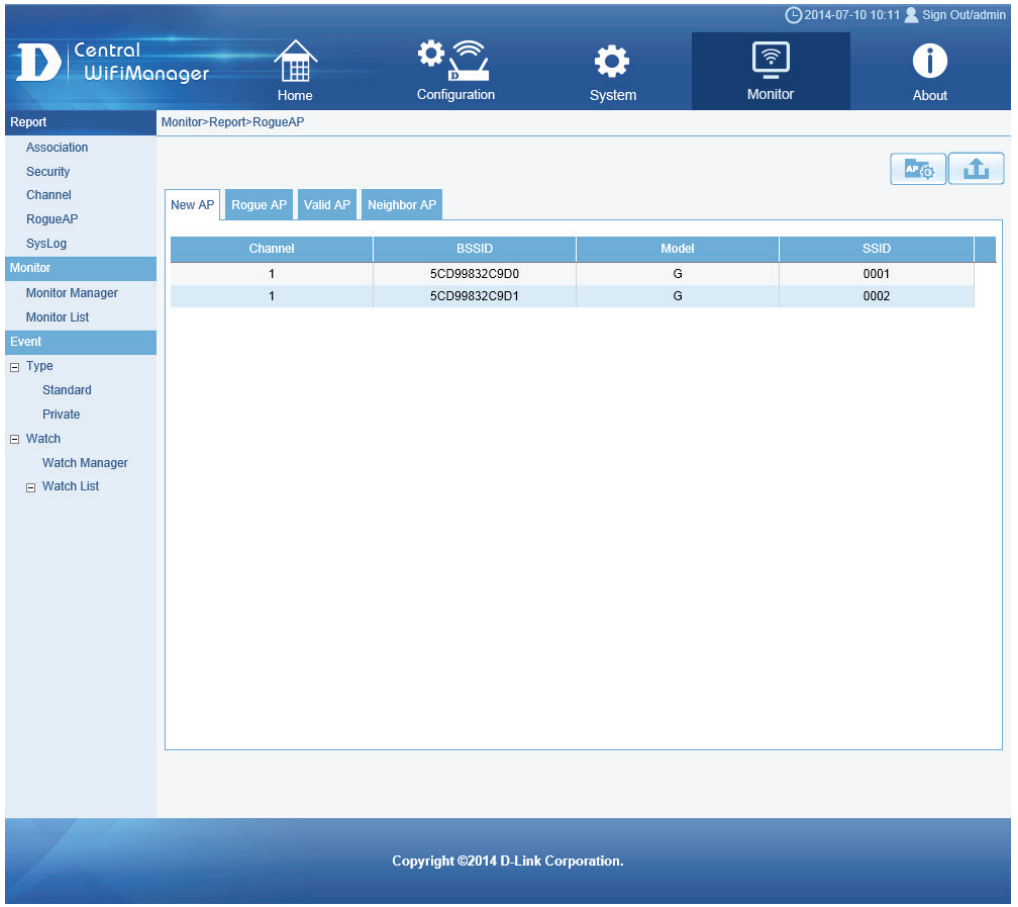
CWM Configuration | Monitor | Report | Rogue AP | New AP

After clicking on **Monitor** in the top panel and **Rogue AP** in the left panel, the following page will be displayed. On this page we can view information about new, rogue, valid and neighboring access points. The purpose of this page is to scan for access points in the network and then to classify them into categories.

In the **New AP** tab, we can view a list of new access points in the environment. Access points displayed here have been detected by access points in our network and were classified as new access points.

Click the button to scan for unclassified access points within the range of the access points connected to our network.

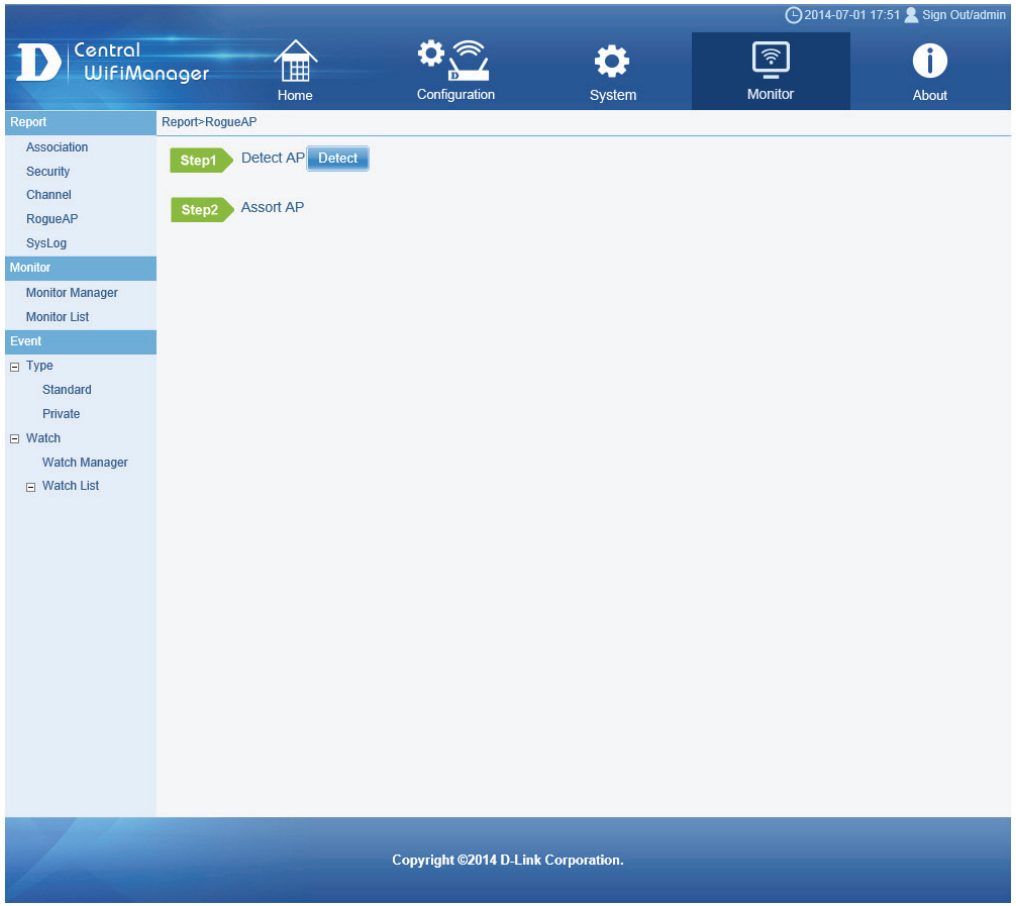
Click the button to export the contents displayed in this table to the computer accessing this interface. This export supports the following file formats; **TXT**, **PDF** and **Excel**.



CWM Configuration | Monitor | Report | Rogue AP | New AP

After clicking the button, the following page will be available. On this page we can initiate a scan for unclassified access points within the wireless range of access points connected to our network.

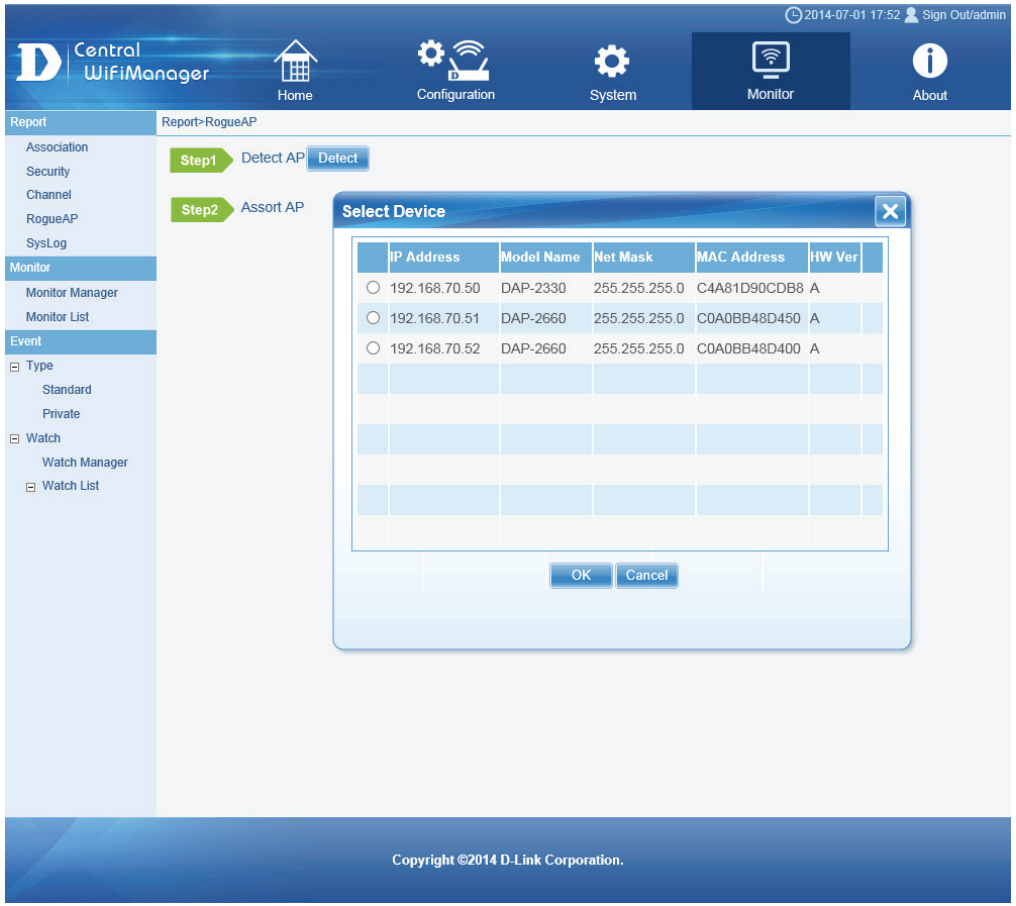
Click the **Detect** button to initiate the scan.



CWM Configuration | Monitor | Report | Rogue AP | New AP

After clicking the **Detect** button, the following page will be available. On this page we can select an access point, in our network, that will be used for the scan.

After selecting an access point, click the **OK** button to start the scan.
Click the **Cancel** button to cancel the scan and return to the main page.

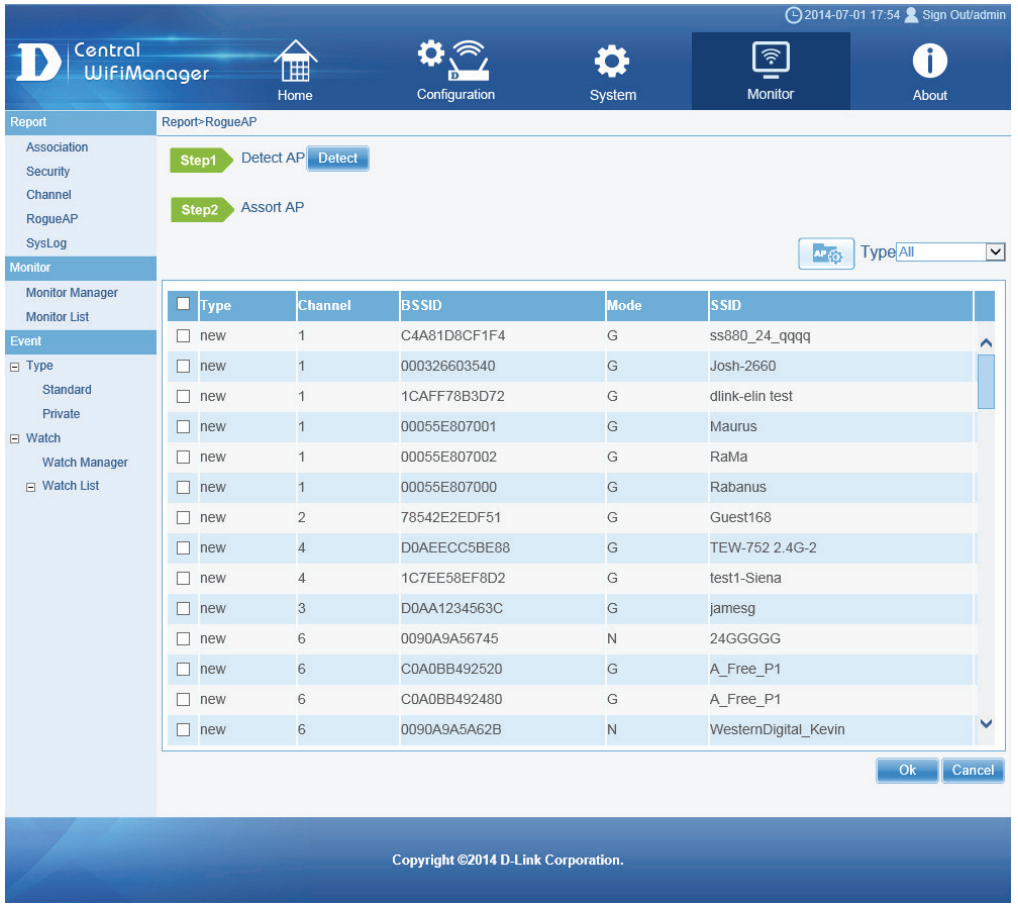


After clicking the **OK** button and after the scan was completed, this page will be available. On this page a list of unclassified access points within the wireless range of the previously select access point in our network will be displayed.

To classify access points in this list, select the check box next to the entry, click the button and select the classification category from the list. Options to choose from are **New**, **Rogue**, **Neighborhood** and **Valid**.

To filter the display entries in the table to only display a certain category, select the **Type** option from the drop-down menu. Filter display options are **All**, **New**, **Rogue**, **Neighborhood** and **Valid**.

Click the **OK** button to classify the selected access points into the category selected. Click the **Cancel** button to cancel the process and return to the main page.

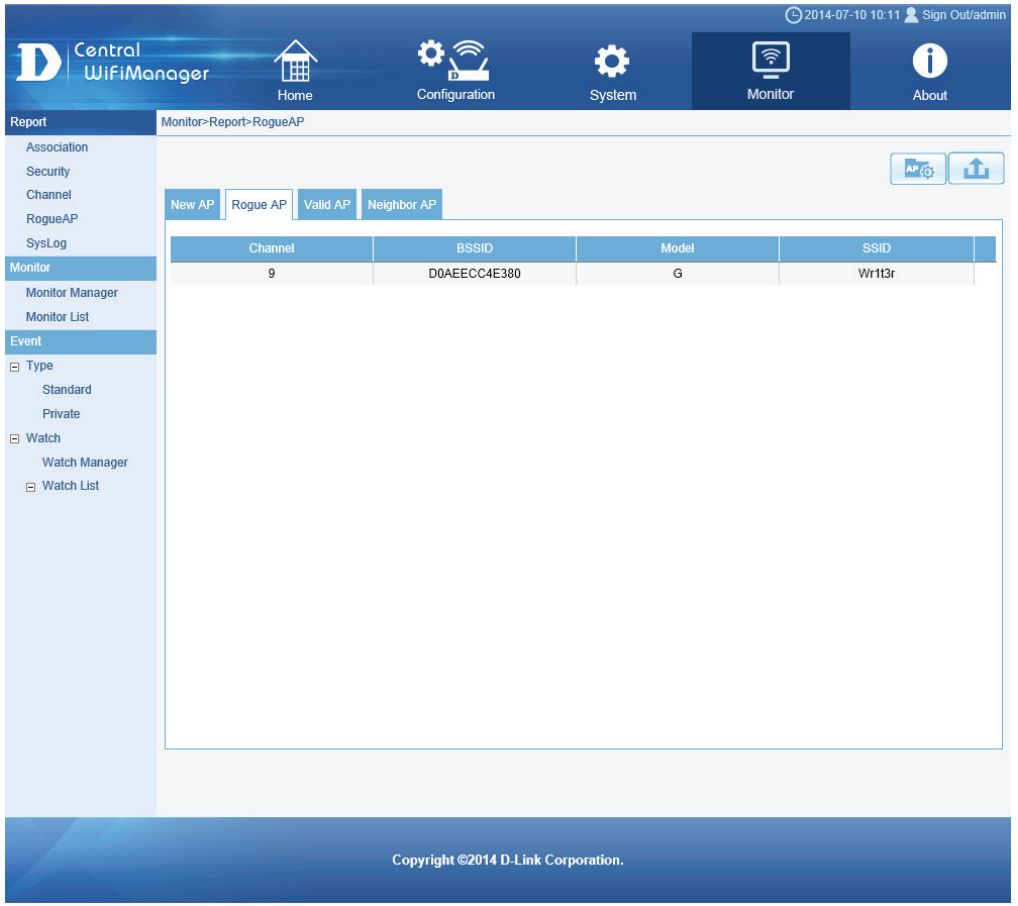


CWM Configuration | Monitor | Report | Rogue AP | **Rogue AP**

In the **Rogue AP** tab, we can view a list of access points in the environment that have been detected by access points in our network and were classified as rogue access points.

Click the button to scan for unclassified access points within the range of the access points connected to our network.

Click the button to export the contents displayed in this table to the computer accessing this interface. This export supports the following file formats; **TXT**, **PDF** and **Excel**.

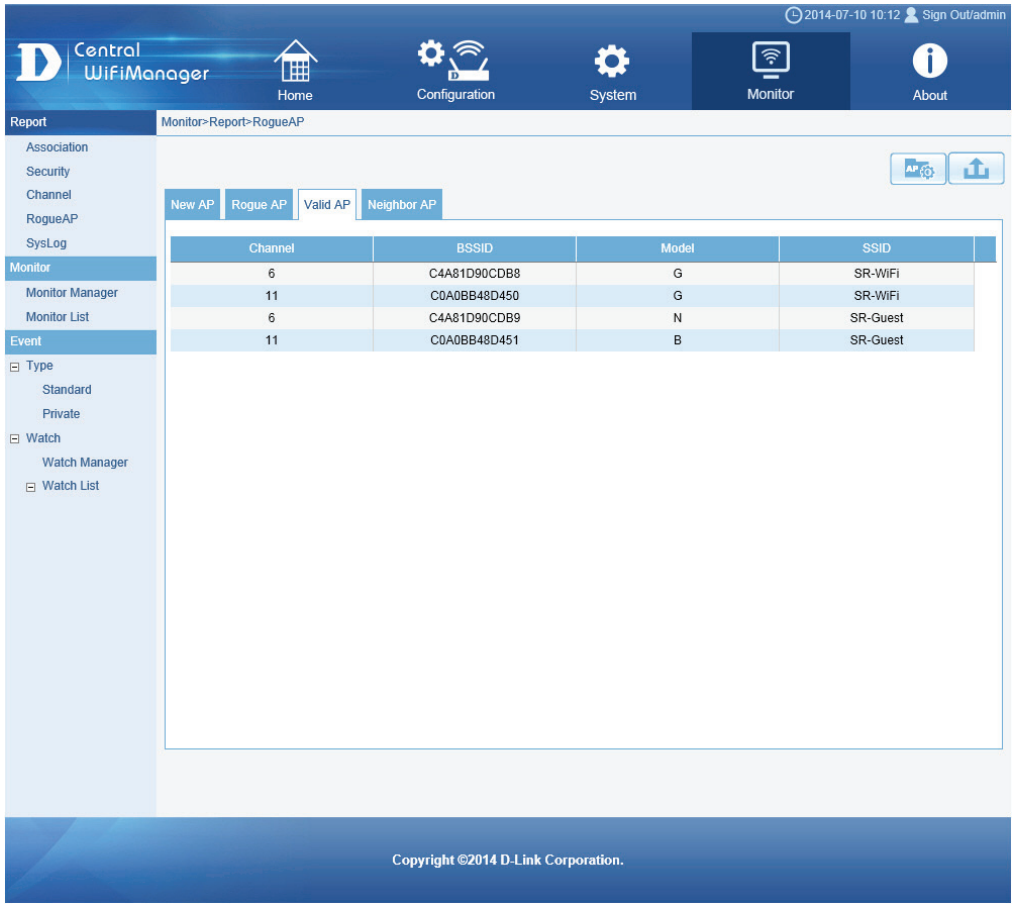


CWM Configuration | Monitor | Report | Rogue AP | **Valid AP**

In the **Valid AP** tab, we can view a list of access points in the environment that have been detected by access points in our network and were classified as valid access points.

Click the button to scan for unclassified access points within the range of the access points connected to our network.

Click the button to export the contents displayed in this table to the computer accessing this interface. This export supports the following file formats; **TXT**, **PDF** and **Excel**.

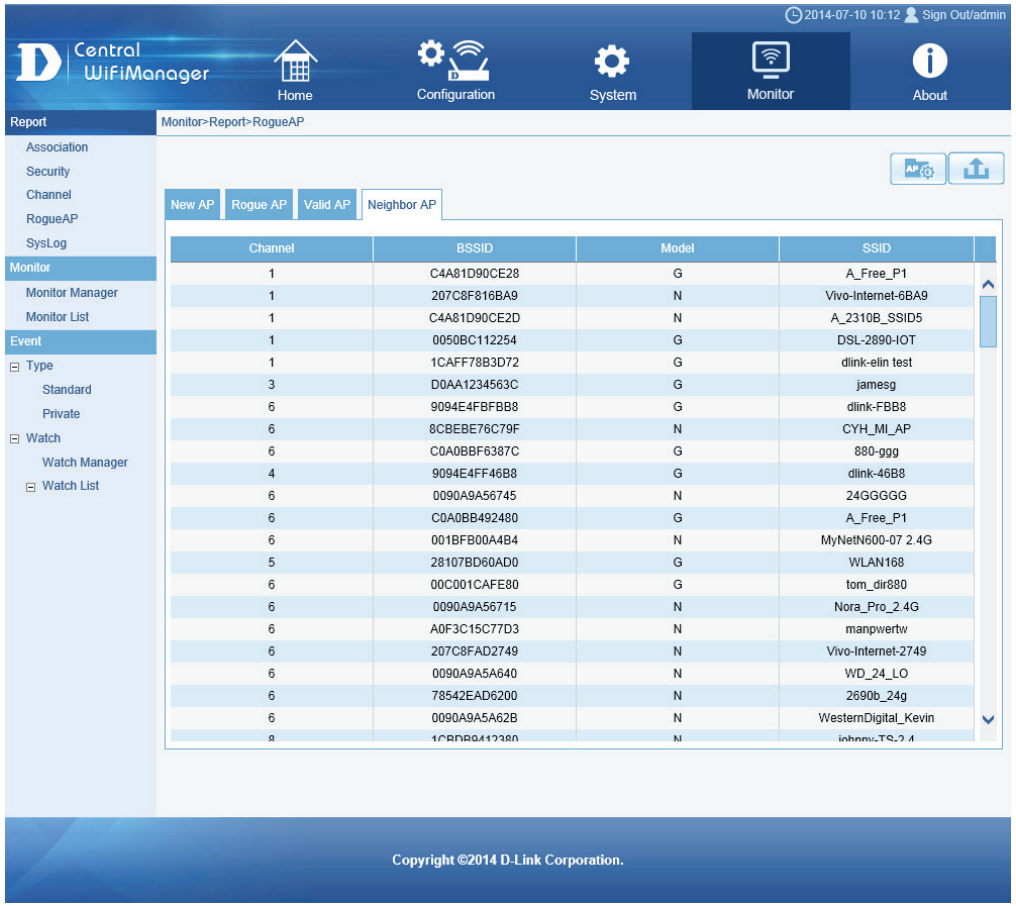


CWM Configuration | Monitor | Report | Rogue AP | **Neighbor AP**

In the **Neighbor AP** tab, we can view a list of access points in the environment that have been detected by access points in our network and were classified as neighbor access points.

Click the button to scan for unclassified access points within the range of the access points connected to our network.

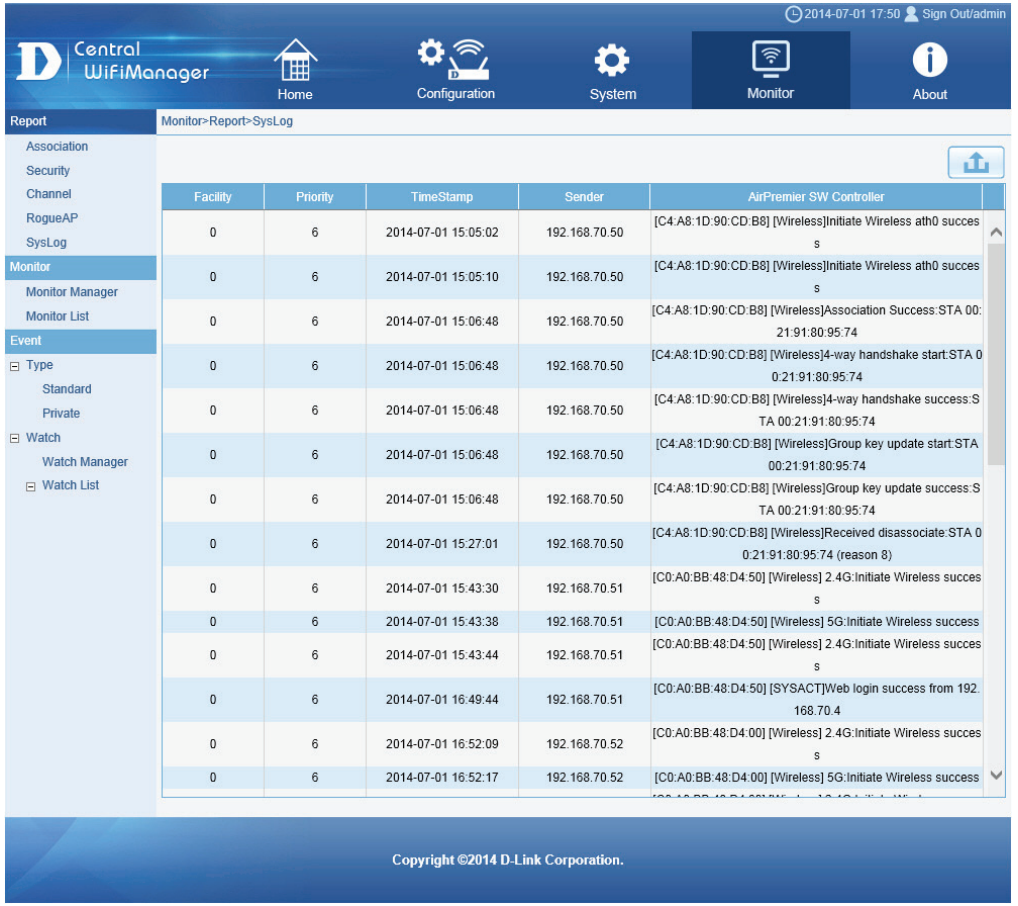
Click the button to export the contents displayed in this table to the computer accessing this interface. This export supports the following file formats; **TXT**, **PDF** and **Excel**.



CWM Configuration | Monitor | Report | SysLog

After clicking on **Monitor** in the top panel and **SysLog** in the left panel, the following page will be displayed. On this page we can view system log entries generated by events that occurred on the network and events that occurred on the Central WifiManager Server application.

Click the button to export the contents displayed in this table to the computer accessing this interface. This export supports the following file formats; **TXT**, **PDF** and **Excel**.

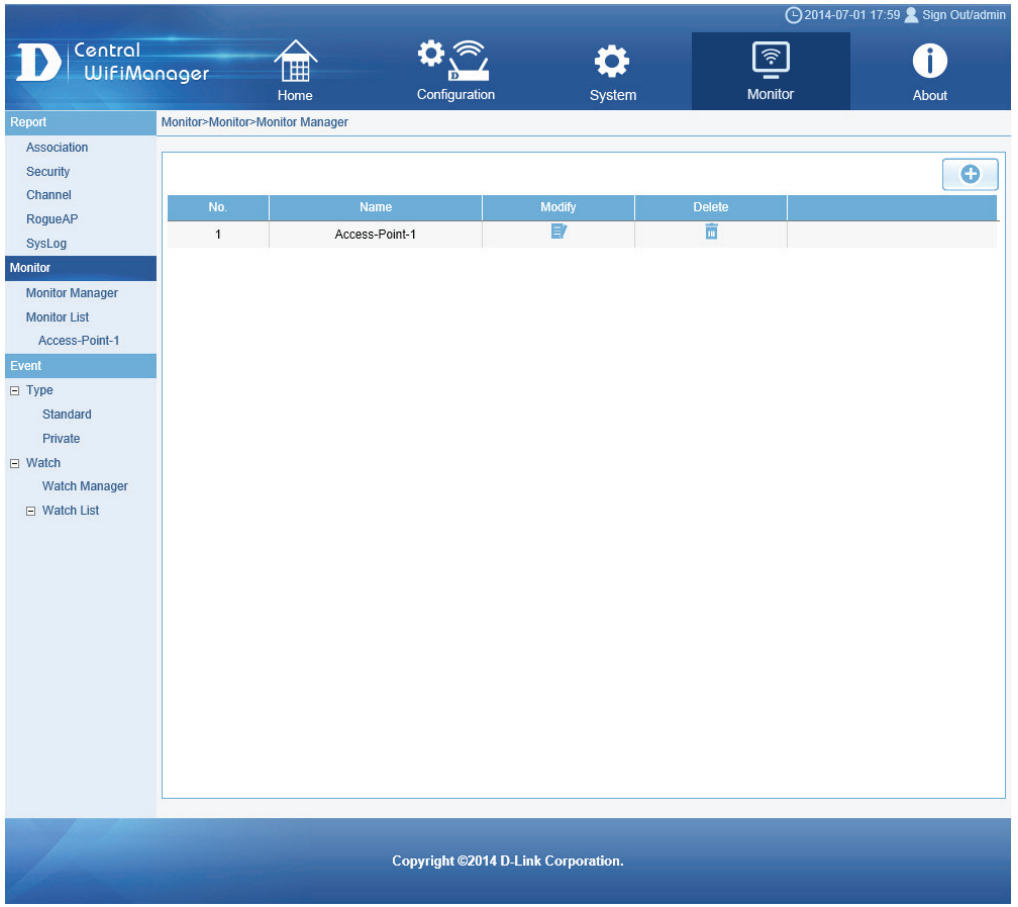

2014-07-01 17:50 Sign Out/admin
Central WifiManager
Home
Configuration
System
Monitor
About
Report
Association
Security
Channel
RogueAP
SysLog
Monitor
Monitor Manager
Monitor List
Event
Type
Standard
Private
Watch
Watch Manager
Watch List
Monitor>Report>SysLog
Facility
Priority
TimeStamp
Sender
AirPremier SW Controller
0 6 2014-07-01 15:05:02 192.168.70.50 [C4:A8:1D:90:CD:B8] [Wireless]Initiate Wireless ath0 success
0 6 2014-07-01 15:05:10 192.168.70.50 [C4:A8:1D:90:CD:B8] [Wireless]Initiate Wireless ath0 success
0 6 2014-07-01 15:06:48 192.168.70.50 [C4:A8:1D:90:CD:B8] [Wireless]Association Success:STA 00:21:91:80:95:74
0 6 2014-07-01 15:06:48 192.168.70.50 [C4:A8:1D:90:CD:B8] [Wireless]4-way handshake start:STA 00:21:91:80:95:74
0 6 2014-07-01 15:06:48 192.168.70.50 [C4:A8:1D:90:CD:B8] [Wireless]4-way handshake success:STA 00:21:91:80:95:74
0 6 2014-07-01 15:06:48 192.168.70.50 [C4:A8:1D:90:CD:B8] [Wireless]Group key update start:STA 00:21:91:80:95:74
0 6 2014-07-01 15:06:48 192.168.70.50 [C4:A8:1D:90:CD:B8] [Wireless]Group key update success:STA 00:21:91:80:95:74
0 6 2014-07-01 15:27:01 192.168.70.50 [C4:A8:1D:90:CD:B8] [Wireless]Received disassociate:STA 00:21:91:80:95:74 (reason 8)
0 6 2014-07-01 15:43:30 192.168.70.51 [C0:A0:BB:48:D4:50] [Wireless] 2.4G:Initiate Wireless success
0 6 2014-07-01 15:43:38 192.168.70.51 [C0:A0:BB:48:D4:50] [Wireless] 5G:Initiate Wireless success
0 6 2014-07-01 15:43:44 192.168.70.51 [C0:A0:BB:48:D4:50] [Wireless] 2.4G:Initiate Wireless success
0 6 2014-07-01 16:49:44 192.168.70.51 [C0:A0:BB:48:D4:50] [SYSACT]Web login success from 192.168.70.4
0 6 2014-07-01 16:52:09 192.168.70.52 [C0:A0:BB:48:D4:00] [Wireless] 2.4G:Initiate Wireless success
0 6 2014-07-01 16:52:17 192.168.70.52 [C0:A0:BB:48:D4:00] [Wireless] 5G:Initiate Wireless success
Copyright ©2014 D-Link Corporation.

CWM Configuration Monitor Monitor Monitor Manager

After clicking on **Monitor** in the top panel and **Monitor Manager** in the left panel, the following page will be displayed. On this page we can view, create and configure monitoring watchdog entries to specifically monitor certain events that take place on certain devices.

On this page, a list of monitor manager watchdog entries are displayed.

Click the button to create a new monitor manager entry.
Click the icon to modify an existing monitor manager entry.
Click the icon to delete an existing monitor manager entry.



CWM Configuration | Monitor | Monitor | Monitor Manager | **Create Profile**

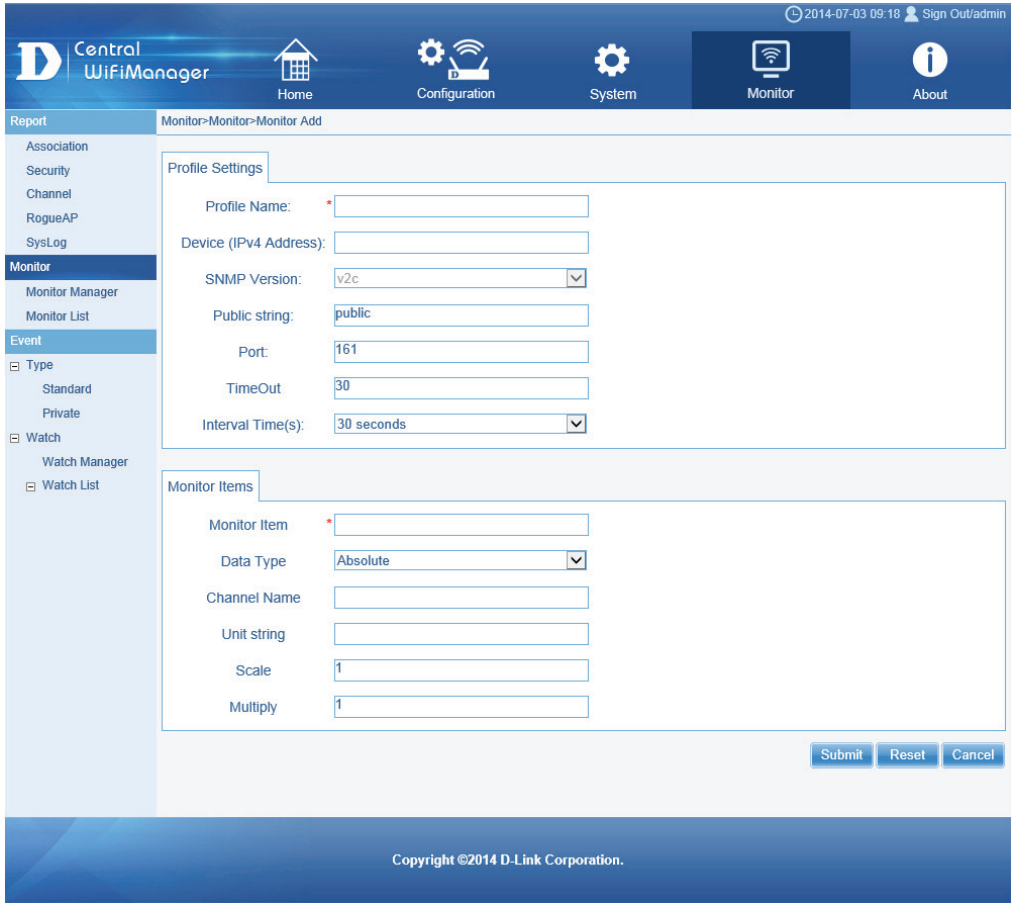
After clicking on the add icon, the following page will be available. On this page we can create or configure a monitor manager watchdog entry.

In the **Profile Settings** section, the following parameters can be configured:

Parameter	Description
Profile Name	Enter the profile name here. This name will be used to identify the entry in the list.
Device (IPv4 Address)	Click in the text box to view a list of access points associated with our network. Select an entry and click **OK** to add it to this field.
SNMP Version	This field will display the SNMP version that will be used for this entry. By default, the version is **SNMPv2c**.
Public String	Enter the public SNMP string name here. By default, this string is **public**.
Port	Enter the port number that the SNMP agent will use to receive request messages. By default, this value is UDP port number 161.
Timeout	Enter the message timeout value here. By default, this value is 30.
Interval Time(s)	Enter the interval time value here. By default, this value is 30 seconds.

In the **Monitor Items** section, the following parameters can be configured:

Parameter	Description
Monitor Item	Click in this text box to view a list of monitor items available for selection. Select a monitor item from the list. Options available for selection are **TransmittedByte-2.4G**, **ReceivedByte-2.4G**, **TransmittedByte-5G**, **ReceivedByte-5G**, and **CPUUtilization**.
Data Type	Select the data type here. Options to choose from are **Absolute** and **Relative**.
Channel Name	Enter the channel name here.
Unit String	Enter the unit string here.
Scale	Enter the scale value here.
Multiply	Enter the multiply value here.



Click the **Submit** button to accept the changes made.
Click the **Reset** button to clear out the information entered in the fields above.
Click the **Cancel** button to discard the changes made and return to the main page.

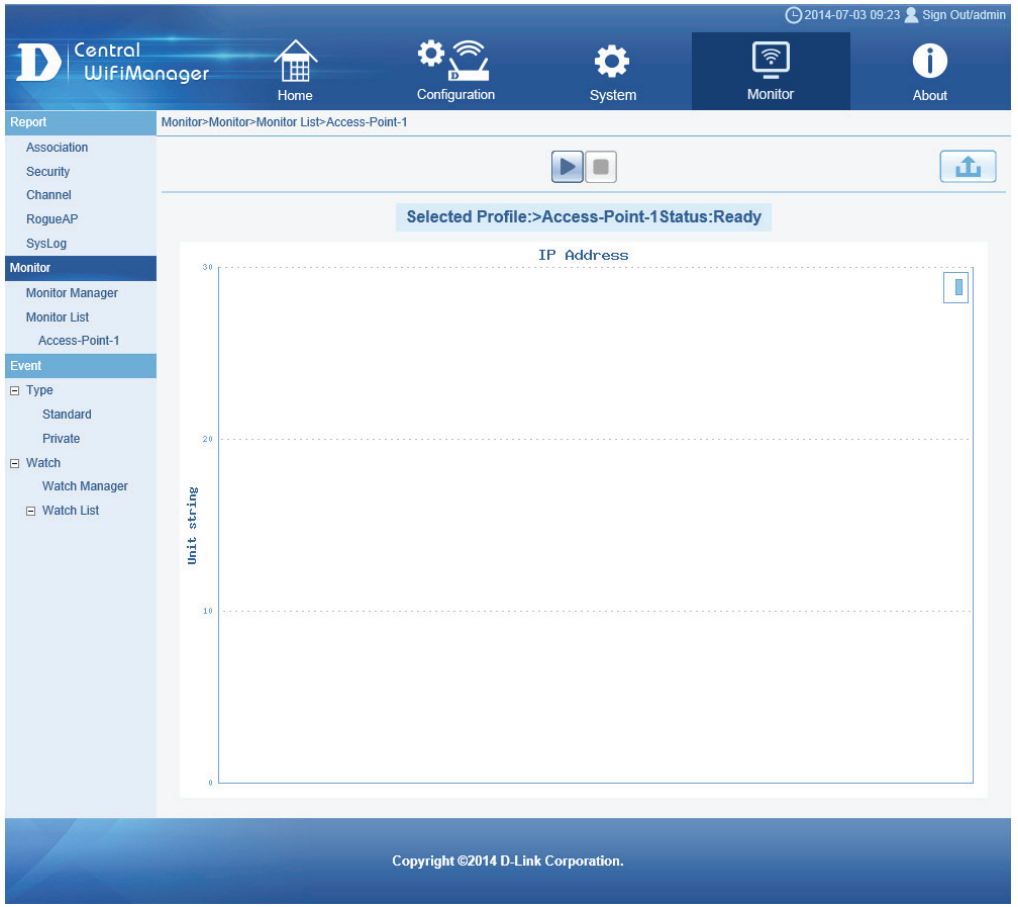
CWM Configuration | Monitor | Monitor | Monitor List

After clicking on **Monitor** in the top panel and **Monitor List** in the left panel, the following page will be displayed. On this page we can view a graphical chart of the monitor manager watchdog events create on the previous page. The list of created events will be displayed under the monitor list option in the left panel.

In this example, we created a monitor manager event called **Access-Point-1**.

Click the button to run the monitor event.
Click the button to stop the monitor event.

Click the button to export the contents displayed in this table to the computer accessing this interface. This export supports the following file format; **PNG**.



CWM Configuration | Monitor | Monitor | Monitor List

After clicking the button, the monitor manager event will run and real-time updates will be displayed in the chart.

In this chart, we monitor the transmitted data of the 2.4GHz frequency band of the access point with the IP address of 192.168.70.50 at 30 second intervals using SNMPv2c and the public string.

Click the button to export this chart. This chart will be exported as an image file with the file format of **PNG**.

Click the button to export the contents displayed in this table to the computer accessing this interface. This export supports the following file format; **PNG**.

CWM Configuration | Monitor | Event | Type | Standard

After clicking on **Monitor** in the top panel and **Event > Type > Standard** in the left panel, the following page will be displayed. On this page we can view standard event type messages generated based on the **Event & Notice Settings** configuration. A standard event is an event that can occur on all devices managed by the Central WifiManager Server application.

In the table, we can choose to display events based on the filtering criteria selected or we can choose to display all events generated.

To filter the events displayed in the table, the following parameters can be configured:

Parameter	Description
Date	Select the starting date by clicking in the first text box available and select the starting date from the option available. Do the same for the ending date selection in the second text box.
Event Level	Select the event level from the drop-down list provided. Options to choose from are **all**, **critic**, **error**, **warning**, and **notice**.
Node IP	Enter the node's IP address here.
Keyword	To display only entries that contain a certain keyword, enter that keyword in this text box.

Click the button to display only the entries based on the criteria entered.

Click the button to display all standard events that have taken place.

Click the button to create a new standard event and notice.

Click the button to export the contents displayed in this table to the computer accessing this interface. This export supports the following file formats; **TXT**, **PDF** and **Excel**.

Click the big button to remove all entries from the event table.

Click the small button next to a specific entry to remove only that entry from the event table.

2014-07-03 09:30
Sign Out/admin
Central WifiManager
Home
Configuration
System
Monitor
About
Report
Association
Security
Channel
RogueAP
SysLog
Monitor
Monitor Manager
Monitor List
Event
Type
Standard
Private
Watch
Watch Manager
Watch List
Monitor>Event
date 2014-07-03 - 2014-07-03 event level: all node IP: keyword:
All
NO. Event Name Event Type Event Date Time Source Description Delete
1 ColdStart standard Trap notice 2014-07-01 15:04:57 192.168.70.50 The sending protocol entity has reinitialized,indicating that the agent's configuration nor entity implementation may be altered.
2 ColdStart standard Trap notice 2014-07-01 15:43:23 192.168.70.51 The sending protocol entity has reinitialized,indicating that the agent's configuration nor entity implementation may be altered.
3 ColdStart standard Trap notice 2014-07-01 16:52:02 192.168.70.52 The sending protocol entity has reinitialized,indicating that the agent's configuration nor entity implementation may be altered.
4 ColdStart standard Trap notice 2014-07-03 09:12:38 192.168.70.51 The sending protocol entity has reinitialized,indicating that the agent's configuration nor entity implementation may be altered.
5 ColdStart standard Trap notice 2014-07-03 09:12:38 192.168.70.52 The sending protocol entity has reinitialized,indicating that the agent's configuration nor entity implementation may be altered.
6 ColdStart standard Trap notice 2014-07-03 09:12:38 192.168.70.50 The sending protocol entity has reinitialized,indicating that the agent's configuration nor entity implementation ma
6 records current page:1/1
Copyright ©2014 D-Link Corporation.

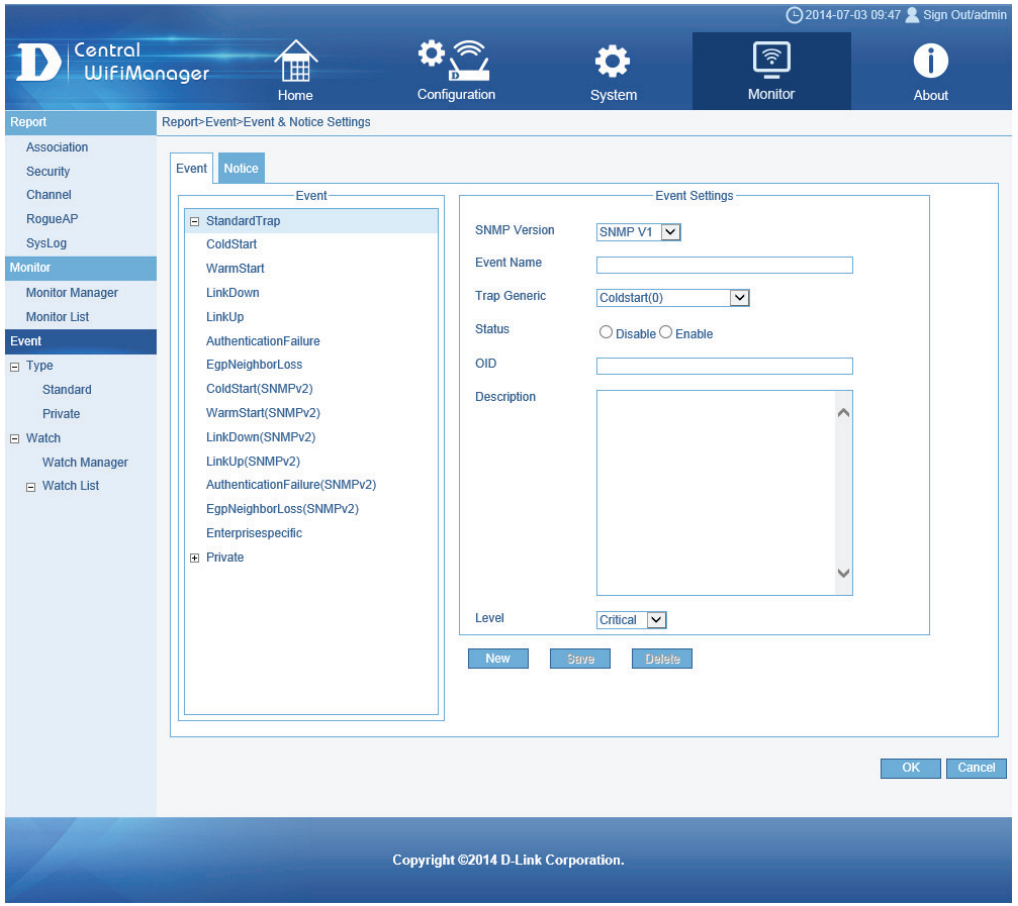
CWM Configuration | Monitor | Event | Type | Standard | **Event**

After clicking the button, the following page will be available. On this page, we can configure the standard SNMP event and notice settings that will be used to display messages on the **Standard** page, when that type of event has occurred on the network. For a complete list of standard traps that are supported by this application, refer to "**Appendix B - Standard & Private Trap List**" on page 105.

In the **Event** tab, the following parameters can be configured:

Parameter	Description
Event	To modify an existing standard trap, select it in this section. After selecting an existing trap, its parameters will automatically be entered in the **Event Settings** section for modification. To create a new trap, do not select any event in this section.
SNMP Version	Select the SNMP version that will be used for this trap here. Options to choose from are **SNMPv1** and **SNMPv2c**. When modifying an existing trap, this field cannot be changed.
Event Name	Enter the event's name here. This name will be used to identify the event in the table mentioned before.
Trap Generic	Select the generic trap that will be used for this new trap here. Options to choose from are **Coldstart(0)**, **WarmStart(1)**, **LinkDown(2)**, **LinkUp(3)**, **AuthenticationFailure(4)**, **EgpNeighborLoss(5)**, and **EnterpriseSpecific(6)**. When modifying an existing trap, this field cannot be changed.
Status	Select to **Enable** or **Disable** this specific trap here.
OID	Enter the Object Identifier (OID) number for this trap here. When modifying an existing trap, this field cannot be changed.
Description	Enter the trap's description here.
Level	Select the level for this trap here. Options to choose from are **Critical**, **Error**, **Warning**, and **Notice**.

Click the **New** button create a new trap event.
Click the **Save** button to accept the changes made.
Click the **Delete** button to delete the selected trap.



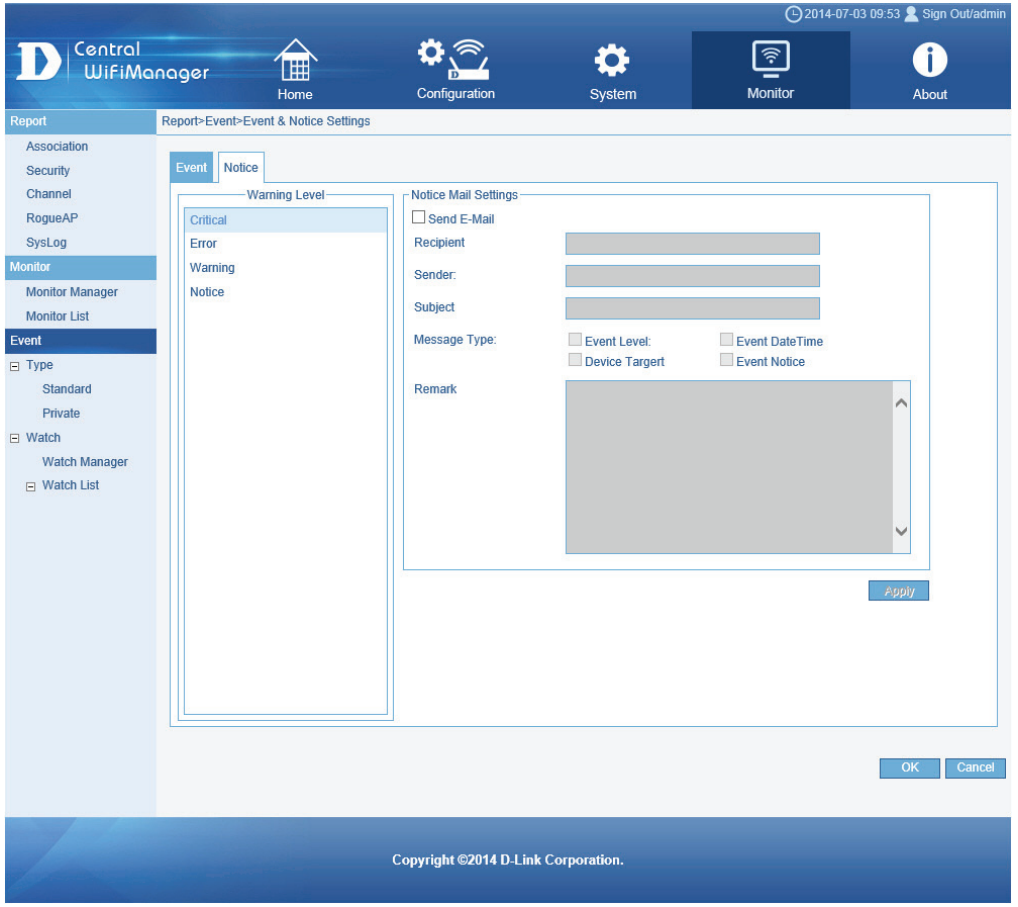
Click the **OK** button to accept the changes made.
Click the **Cancel** button to discard the changes made and return to the main page.

CWM Configuration | Monitor | Event | Type | Standard | **Notice**

In the **Notice** tab, we can enable the notification feature when a standard trap event was generated for a specific warning level.

The following parameters can be configured:

Parameter	Description
Warning Level	Select the warning level here. Options to choose from are **Critical**, **Error**, **Warning**, and **Notice**.
Send E-Mail	After the warning level was selected, select this option to enable the email notification feature for the selected warning level.
Recipient	Enter the recipient's email address here.
Sender	Enter the sender's email address here.
Subject	Enter the subject for the message here.
Message Type	Select the message type here. Options to choose from are **Event Level**, **Event Date/Time**, **Device Target**, and **Event Notice**.
Remark	Enter the remark for this message here.



Click the **Apply** button to accept the changes made.

Click the **OK** button to accept the changes made.
Click the **Cancel** button to discard the changes made and return to the main page.

CWM Configuration | Monitor | Event | Type | Private

After clicking on **Monitor** in the top panel and **Event > Type > Private** in the left panel, the following page will be displayed. On this page we can view private event type messages generated based on the **Event & Notice Settings** configuration. A private event is an event that can only occur on specific devices that are managed by the Central WifiManager Server application. These events are product specific. For a complete list of private traps that are supported by this application, refer to "**Appendix B - Standard & Private Trap List**" on page 105.

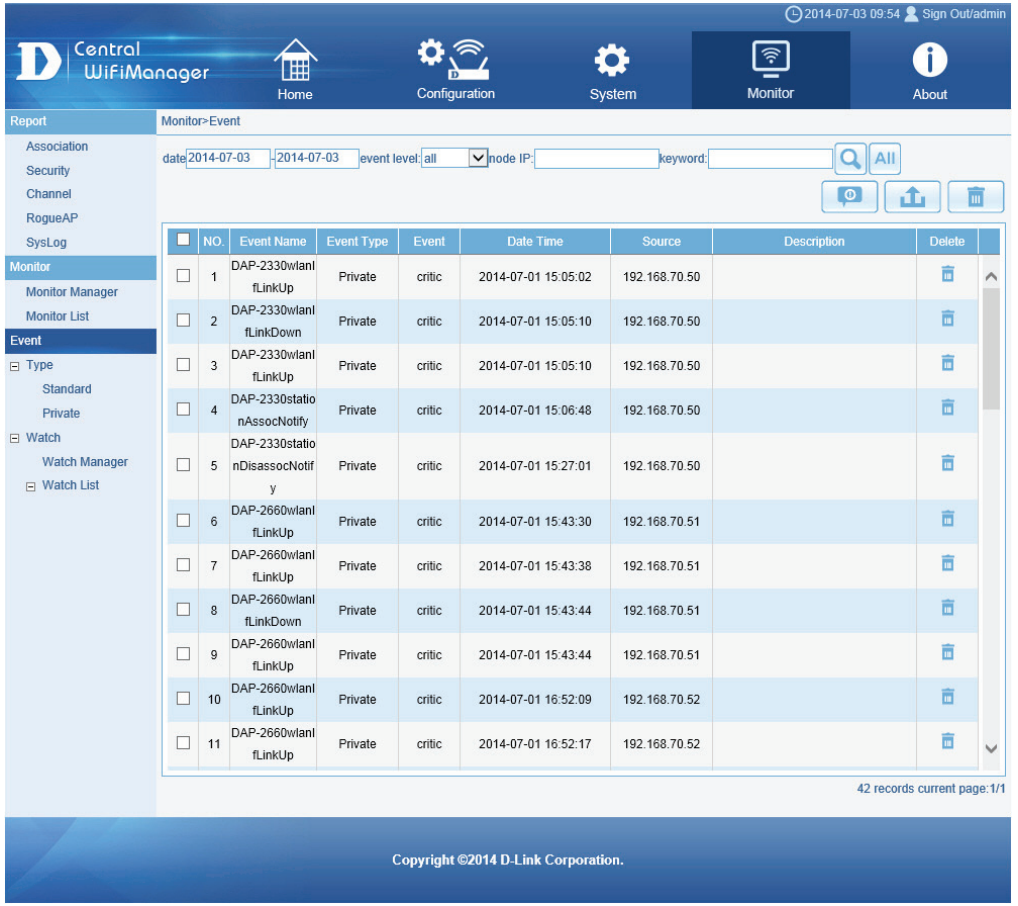
In the table, we can choose to display events based on the filtering criteria selected or we can choose to display all events generated.

To filter the events displayed in the table, the following parameters can be configured:

Parameter	Description
Date	Select the starting date by clicking in the first text box available and select the starting date from the option available. Do the same for the ending date selection in the second text box.
Event Level	Select the event level from the drop-down list provided. Options to choose from are **all**, **critic**, **error**, **warning**, and **notice**.
Node IP	Enter the node's IP address here.
Keyword	To display only entries that contain a certain keyword, enter that keyword in this text box.

Click the button to display only the entries based on the criteria entered.
Click the button to display all private events that have taken place.

Click the button to create a new private event and notice.
Click the button to export the contents displayed in this table to the computer accessing this interface. This export supports the following file formats; **TXT**, **PDF** and **Excel**.
Click the big button to remove all entries from the event table.
Click the small button next to a specific entry to remove only that entry from the event table.

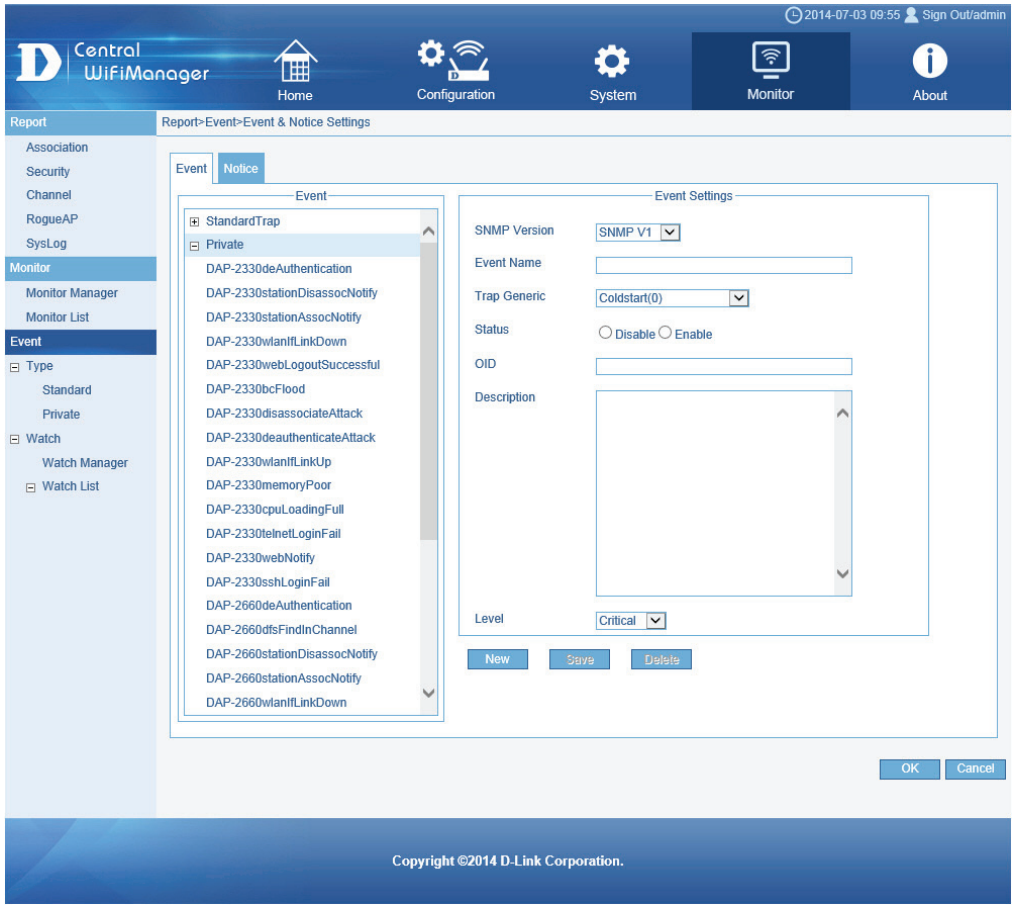


CWM Configuration | Monitor | Event | Type | Private | Event

After clicking the button, the following page will be available. On this page, we can configure the private SNMP event and notice settings that will be used to display messages on the **Private** page, when that type of event has occurred on the network.

In the **Event** tab, the following parameters can be configured:

Parameter	Description
Event	To modify an existing private trap, select it in this section. After selecting an existing trap, its parameters will automatically be entered in the **Event Settings** section for modification. To create a new trap, do not select any event in this section.
SNMP Version	Select the SNMP version that will be used for this trap here. Options to choose from are **SNMPv1** and **SNMPv2c**. When modifying an existing trap, this field cannot be changed.
Event Name	Enter the event's name here. This name will be used to identify the event in the table mentioned before.
Trap Generic	Select the generic trap that will be used for this new trap here. Options to choose from are **Coldstart(0)**, **WarmStart(1)**, **LinkDown(2)**, **LinkUp(3)**, **AuthenticationFailure(4)**, **EgpNeighborLoss(5)**, and **EnterpriseSpecific(6)**. When modifying an existing trap, this field cannot be changed.
Status	Select to **Enable** or **Disable** this specific trap here.
OID	Enter the Object Identifier (OID) number for this trap here. When modifying an existing trap, this field cannot be changed.
Description	Enter the trap's description here.
Level	Select the level for this trap here. Options to choose from are **Critical**, **Error**, **Warning**, and **Notice**.



Click the **New** button create a new trap event.
Click the **Save** button to accept the changes made.
Click the **Delete** button to delete the selected trap.

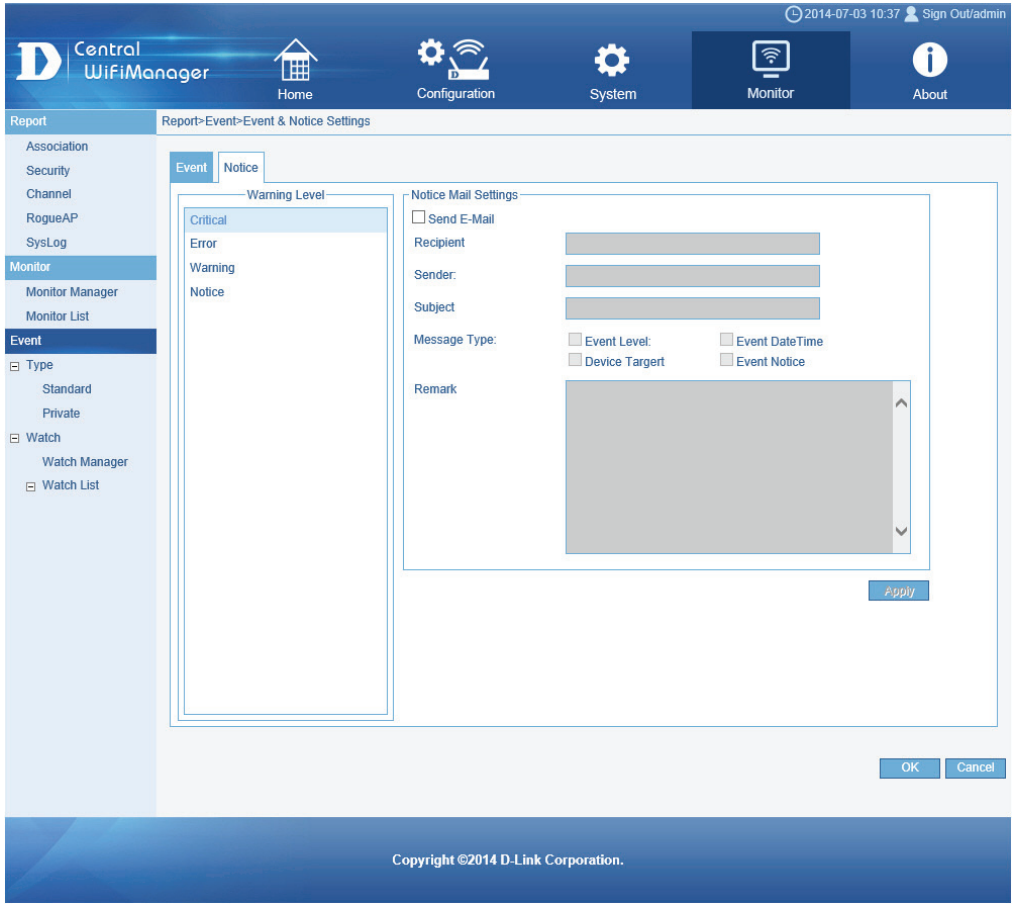
Click the **OK** button to accept the changes made.
Click the **Cancel** button to discard the changes made and return to the main page.

CWM Configuration | Monitor | Event | Type | Private | Notice

In the **Notice** tab, we can enable the notification feature when a private trap event was generated for a specific warning level.

The following parameters can be configured:

Parameter	Description
Warning Level	Select the warning level here. Options to choose from are **Critical**, **Error**, **Warning**, and **Notice**.
Send E-Mail	After the warning level was selected, select this option to enable the email notification feature for the selected warning level.
Recipient	Enter the recipient's email address here.
Sender	Enter the sender's email address here.
Subject	Enter the subject for the message here.
Message Type	Select the message type here. Options to choose from are **Event Level**, **Event Date/Time**, **Device Target**, and **Event Notice**.
Remark	Enter the remark for this message here.



Click the **Apply** button to accept the changes made.

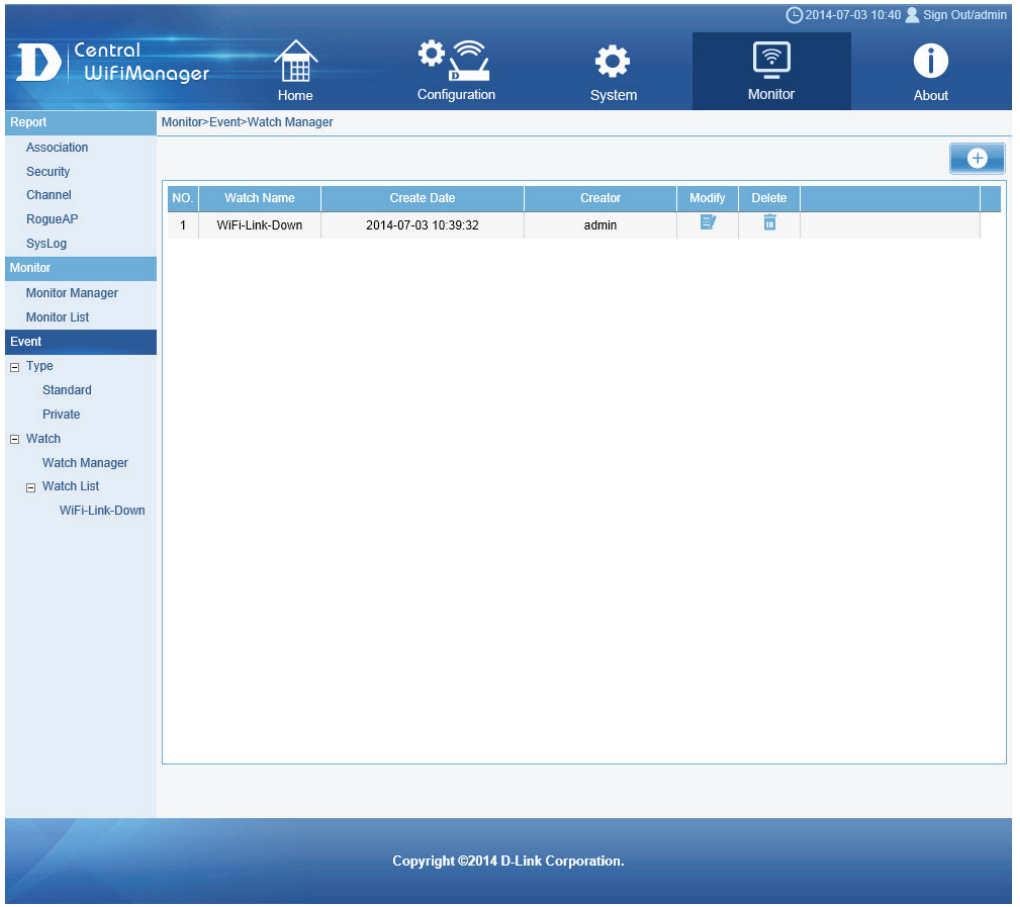
Click the **OK** button to accept the changes made.
Click the **Cancel** button to discard the changes made and return to the main page.

CWM Configuration | Monitor | Event | Watch | **Watch Manager**

After clicking on **Monitor** in the top panel and **Event > Watch > Watch Manager** in the left panel, the following page will be displayed. On this page we can view, create and configure watch manager profiles.

Existing watch manager profiles are displayed in the table on this page.

Click the button to create a new watch manager profile.
Click the icon to modify an existing watch manager profile.
Click the icon to delete an existing watch manager profile.



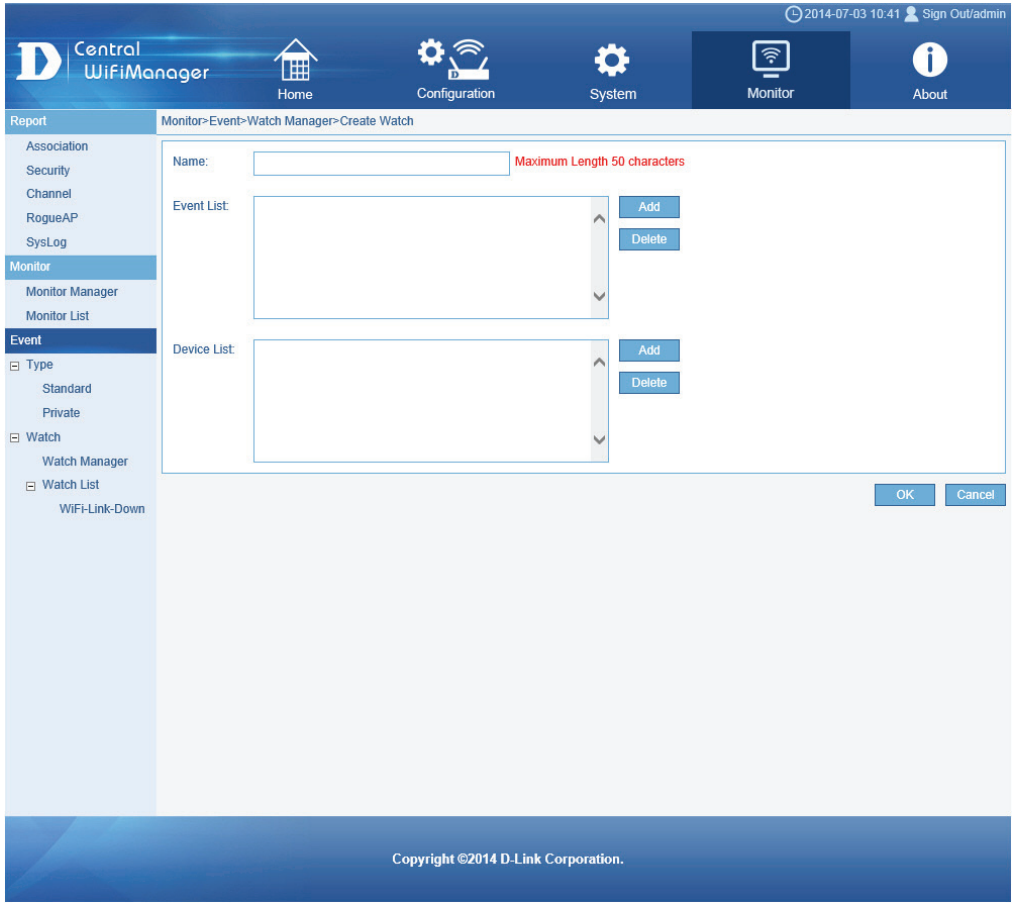
CWM Configuration | Monitor | Event | Watch | Watch Manager | **Create Watch**

After clicking the button, the following page will be available. On this page we can create a new watch manager profile.

The following parameters can be configured:

Parameter	Description
Name	Enter the watch manager profile's name here.
Event List	To add an event to the event list, click on the **Add** button. To remove an event from the event list, select it and click on the **Delete** button.
Device List	To add a device to the device list, click on the **Add** button. To remove a device from the device list, select it and click on the **Delete** button.

Click the **OK** button to accept the changes made.
Click the **Cancel** button to discard the changes made and return to the main page.



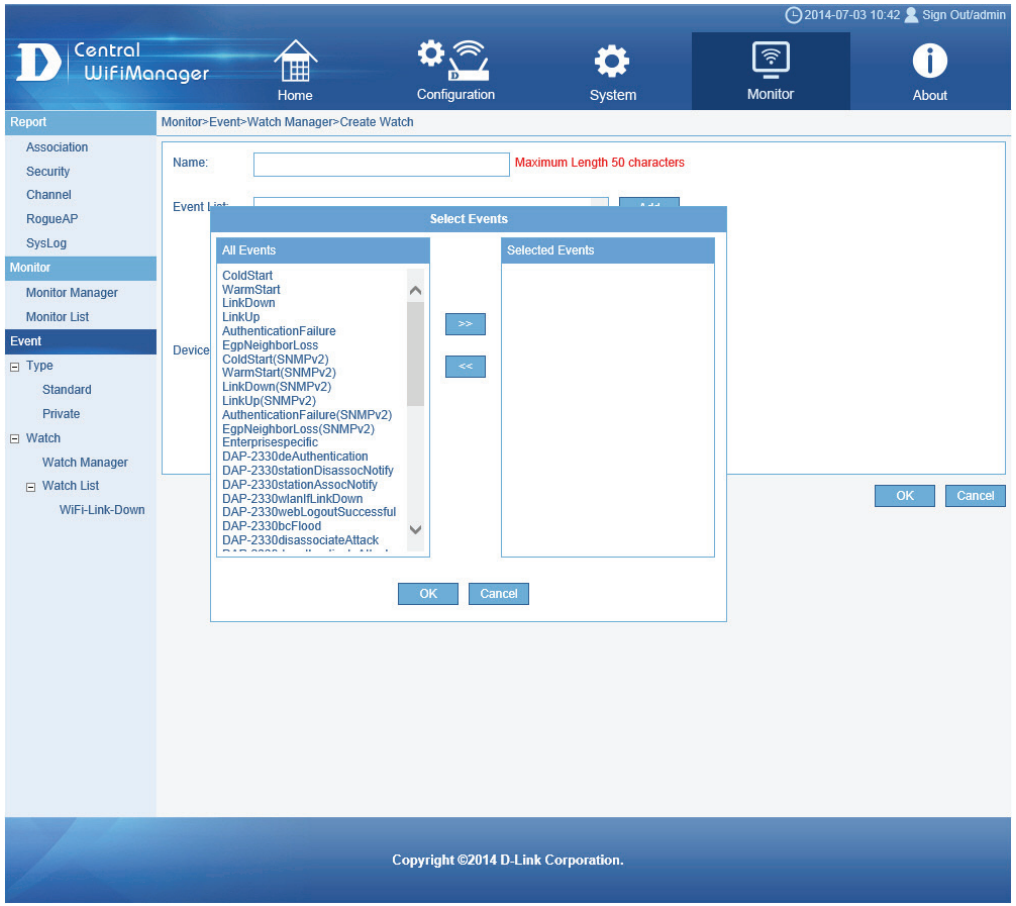
CWM Configuration | Monitor | Event | Watch | Watch Manager | **Create Watch**

After clicking the **Add** button next to the **Event List** parameter, the following window will appear.

In the **All Event** section, all available trap events will be displayed.

To use one or more of these events, select them and click on the **>>** button add them to the **Selected Event** section.
To remove one or more of the selected events from the **Selected Events** section, select them and click on the **<<** button.

Click the **OK** button to accept the selections made.
Click the **Cancel** button to discard the selections made and return to the previous page.

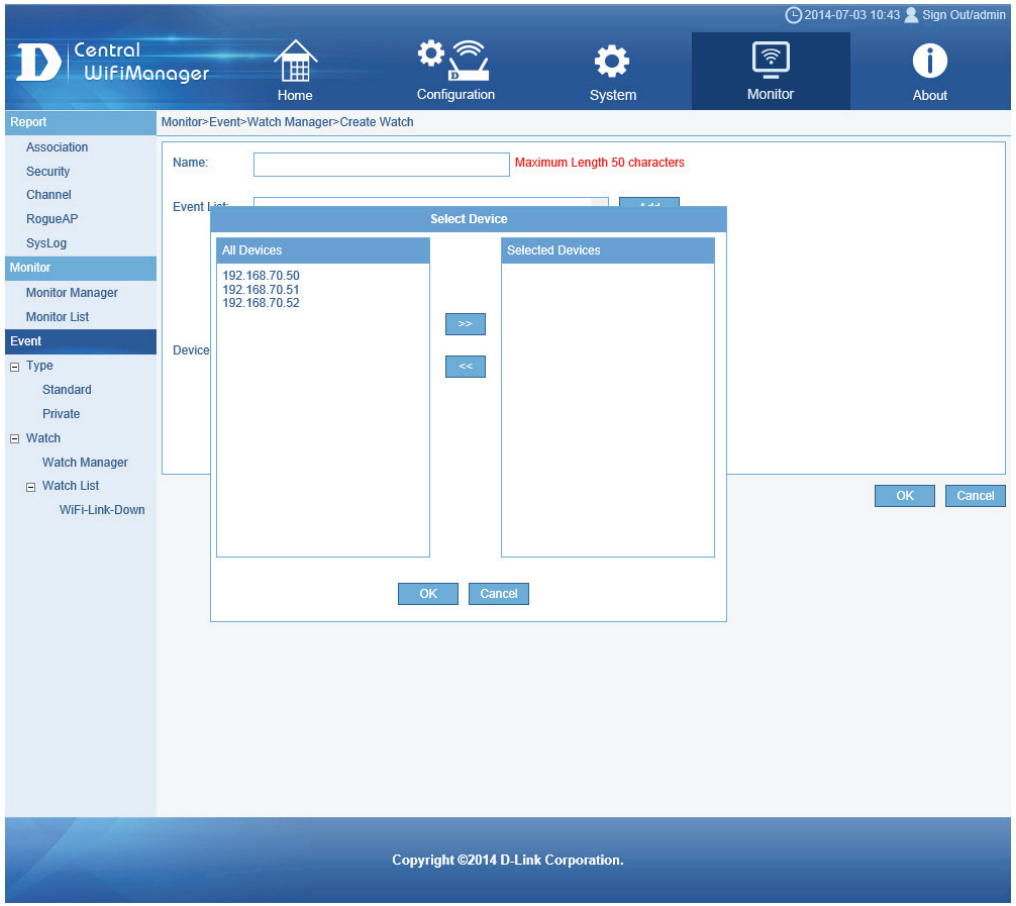


After clicking the **Add** button next to the **Device List** parameter, the following window will appear.

In the **All Device** section, all available access points in the network, managed by this application, will be displayed.

To use one or more of these devices, select them and click on the **>>** button add them to the **Selected Devices** section.
To remove one or more of the selected devices from the **Selected Devices** section, select them and click on the **<<** button.

Click the **OK** button to accept the selections made.
Click the **Cancel** button to discard the selections made and return to the previous page.

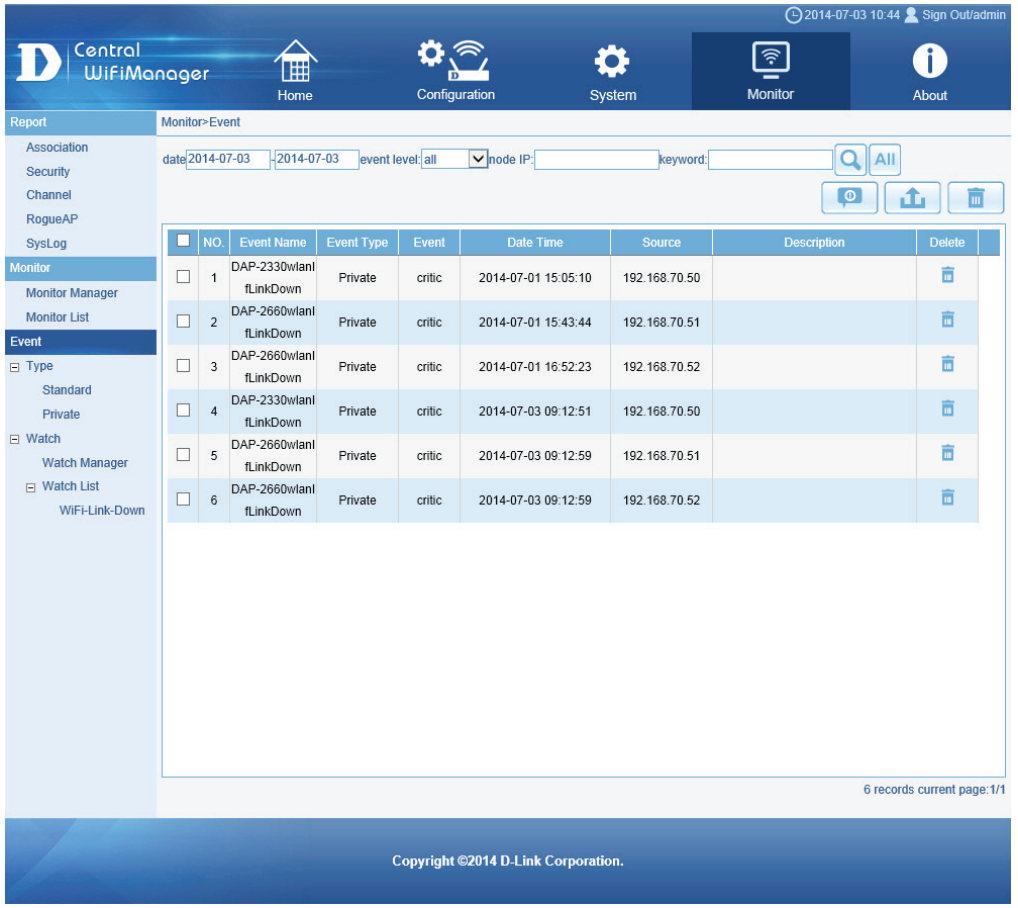


CWM Configuration | Monitor | Event | Watch | **Watch List**

After creating watch manager profiles in the previous section, those profiles will be available for selection under the **Watch List** option in the left panel. In this example, we created a watch manager profile called **WiFi-Link-Down** that will generate events when an access point in this network's wireless link goes down. After clicking on **Monitor** in the top panel and **Event > Watch > Watch List > WiFi-Link-Down** in the left panel, the following page will be displayed. On this page we can view watch list messages that were generated based on the watch manager profile's settings.

To filter the messages displayed in this table, the following parameters can be configured:

Parameter	Description
Date	Select the starting date by clicking in the first text box available and select the starting date from the option available. Do the same for the ending date selection in the second text box.
Event Level	Select the event level from the drop-down list provided. Options to choose from are **all**, **critic**, **error**, **warning**, and **notice**.
Node IP	Enter the node's IP address here.
Keyword	To display only entries that contain a certain keyword, enter that keyword in this text box.



Click the button to display only the entries based on the criteria entered.

Click the button to display all private events that have taken place.

Click the button to create a new event and notice.

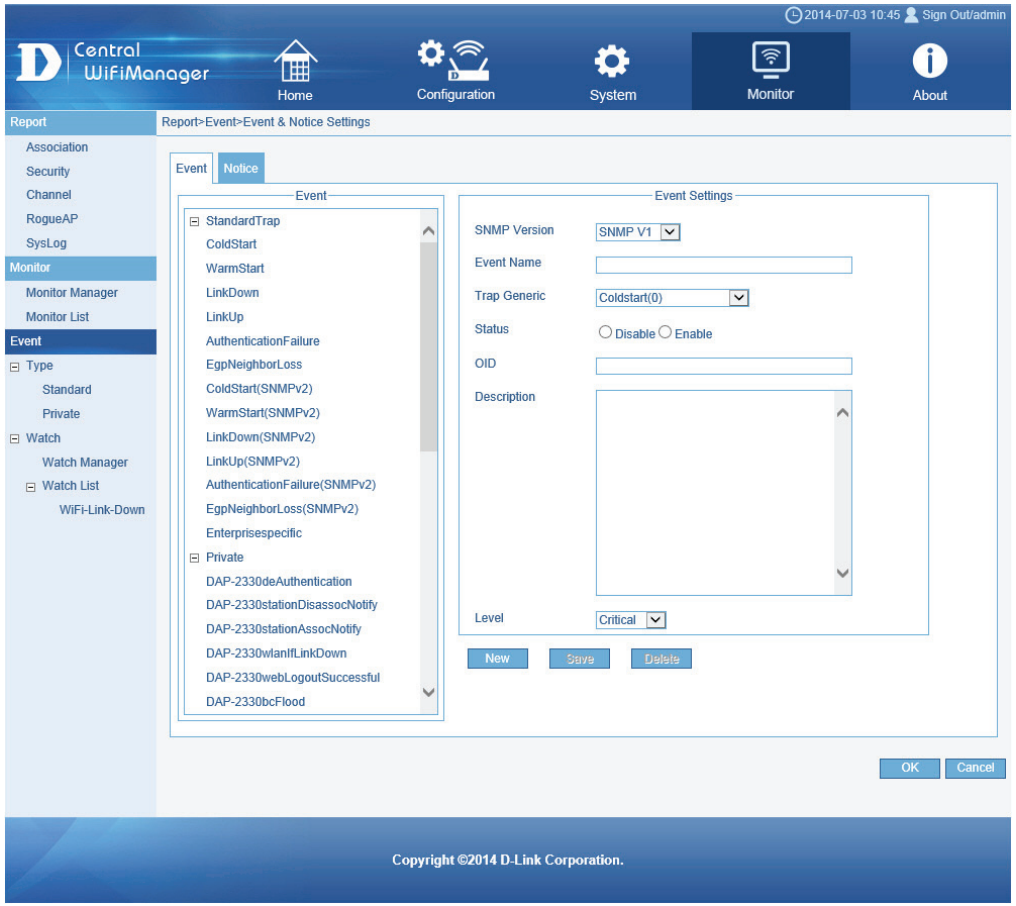
Click the button to export the contents displayed in this table to the computer accessing this interface. This export supports the following file formats; **TXT**, **PDF** and **Excel**.

Click the big button to remove all entries from the event table.

Click the small button next to a specific entry to remove only that entry from the event table.

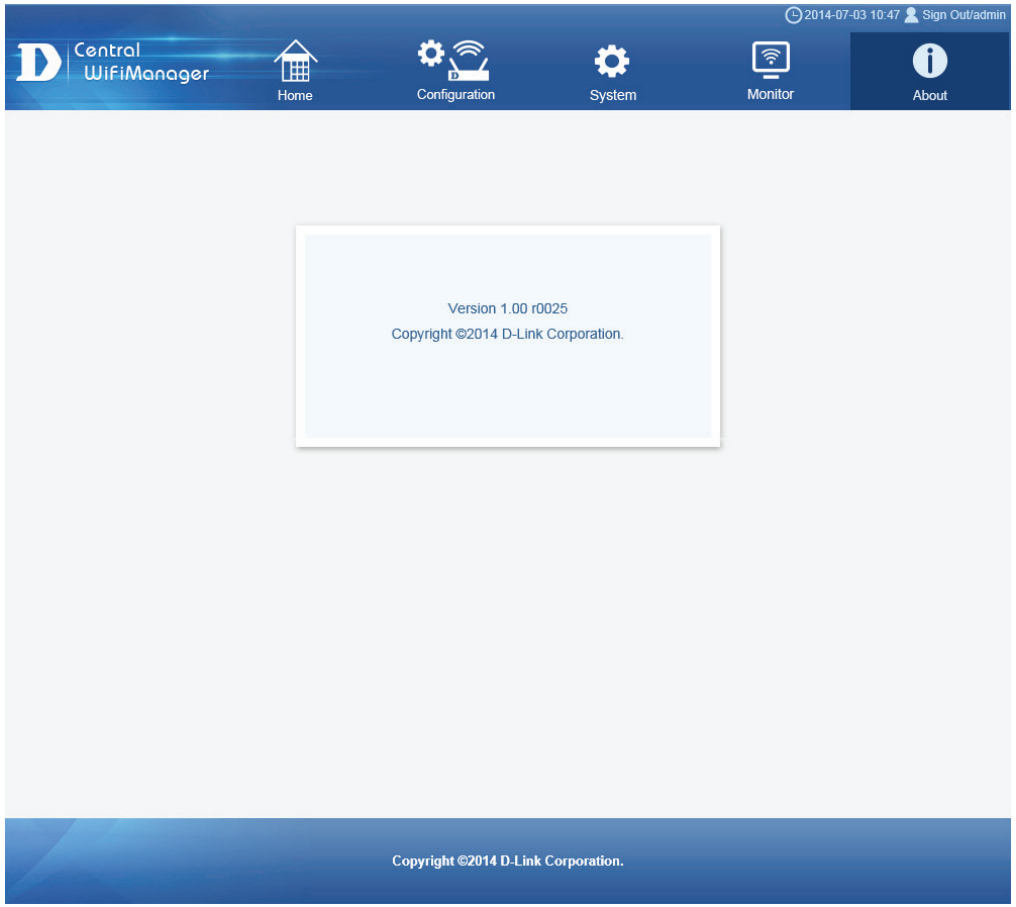
CWM Configuration | Monitor | Event | Watch | **Watch List**

To create or configure standard SNMP event and notice settings, refer to “**Standard**” on page 82.
To create or configure private SNMP event and notice settings, refer to “**Private**” on page 85.



CWM Configuration About

After clicking on **About** in the top panel, the following page will be displayed. On this page we can view the version number and copyright notice of the Central WifiManager Server application.

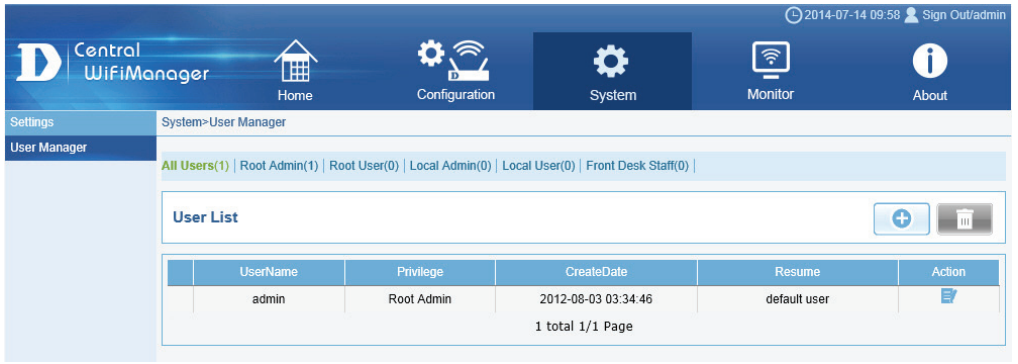


Appendix A - Front Desk Staff & User Access

Front desk user accounts can be created to allow guests to use the wireless network for a limited amount of time. Normally, restricted wireless access is given to front desk wireless users. In this section we'll discuss how to create and use a front desk staff account and how generate guest pass codes.

To setup a **front desk staff** account, we need to enter the Central WifiManager Server application with an administrative account. Navigate to **System**, in the top menu, and **User Manager**, in the left menu.

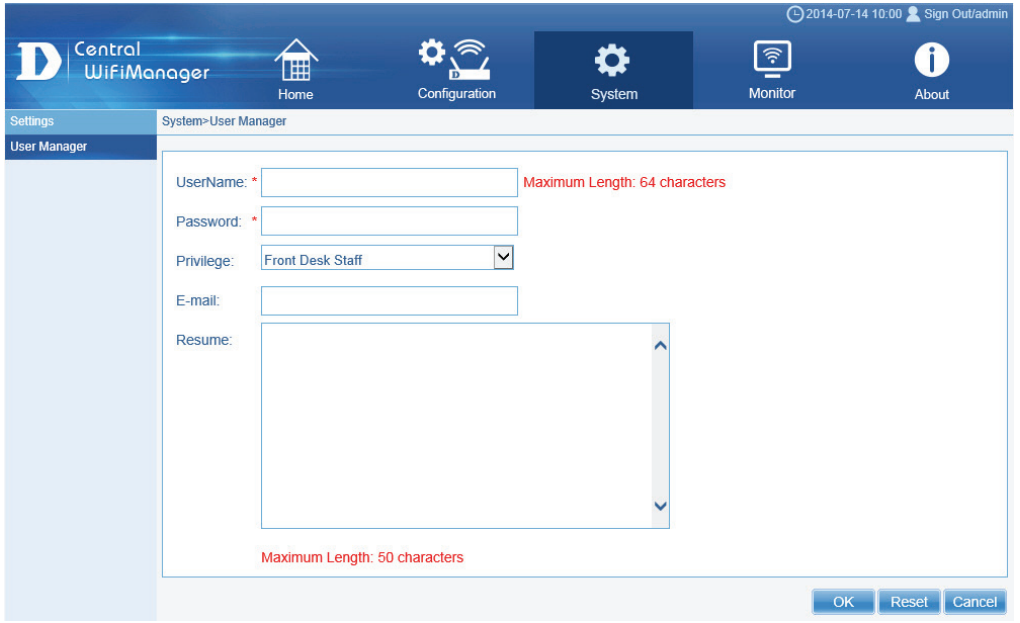
Click the button, to create a new user account.



After clicking the button, the following page will be available. The following parameters can be configured:

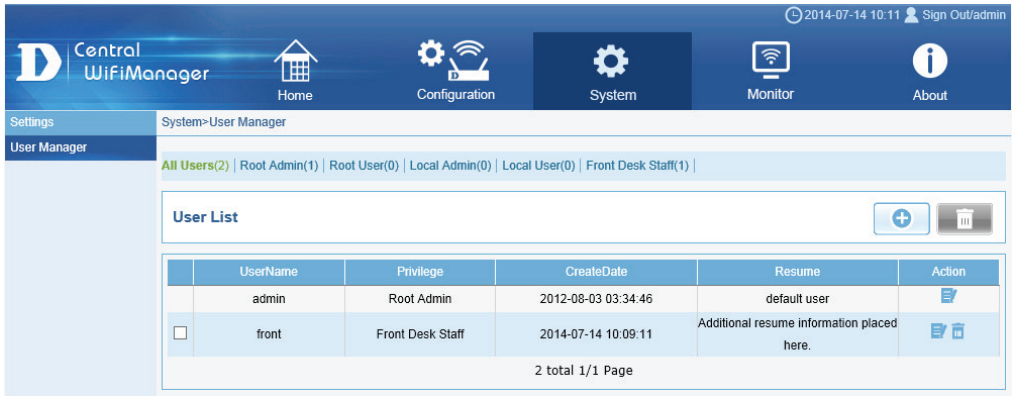
Parameter	Description
Username	Enter the front desk staff account's username here.
Password	Enter the front desk staff account's password here.
Privilege	Select the **Front Desk Staff** option here.
E-mail	Enter the front desk staff person's email address here.
Resume	Enter additional information about this account here.

Click the **OK** button to create the new account.
Click the **Reset** button to clear out the information entered in the fields.



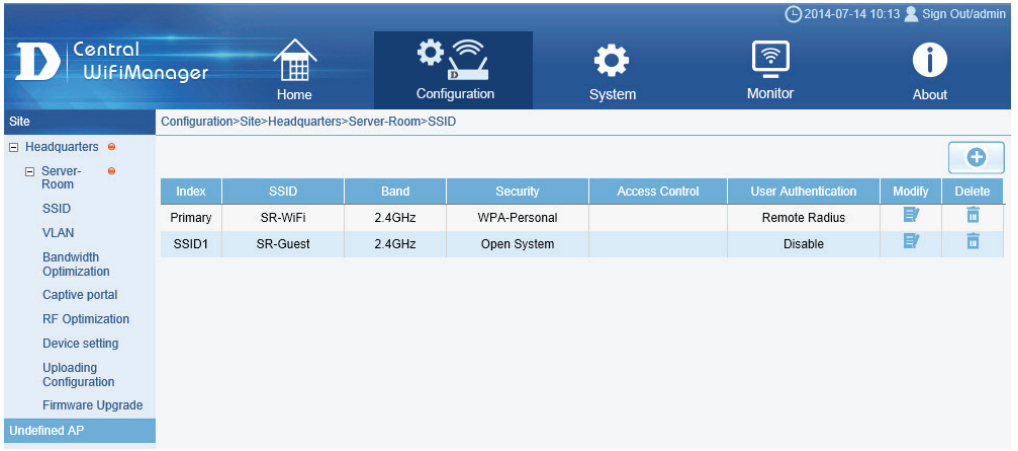
Appendix A - Front Desk Staff & User Access

After successfully adding the front desk staff account, it will be displayed in the user manager table.


2014-07-14 10:11 Sign Out/admin
Central WifiManager
Home
Configuration
System
Monitor
About
Settings
User Manager
System>User Manager
All Users(2) | Root Admin(1) | Root User(0) | Local Admin(0) | Local User(0) | Front Desk Staff(1) |
User List
UserName Privilege CreateDate Resume Action
admin Root Admin 2012-08-03 03:34:46 default user
front Front Desk Staff 2014-07-14 10:09:11 Additional resume information placed here.
2 total 1/1 Page

In the next step we need configure our guest wireless network to use pass codes for user authentication. Navigate to **Configuration**, in the top menu, and select your network, in the left menu. In our example, the guest network is located within the **Server-Room** network, at the **Headquarters** site.

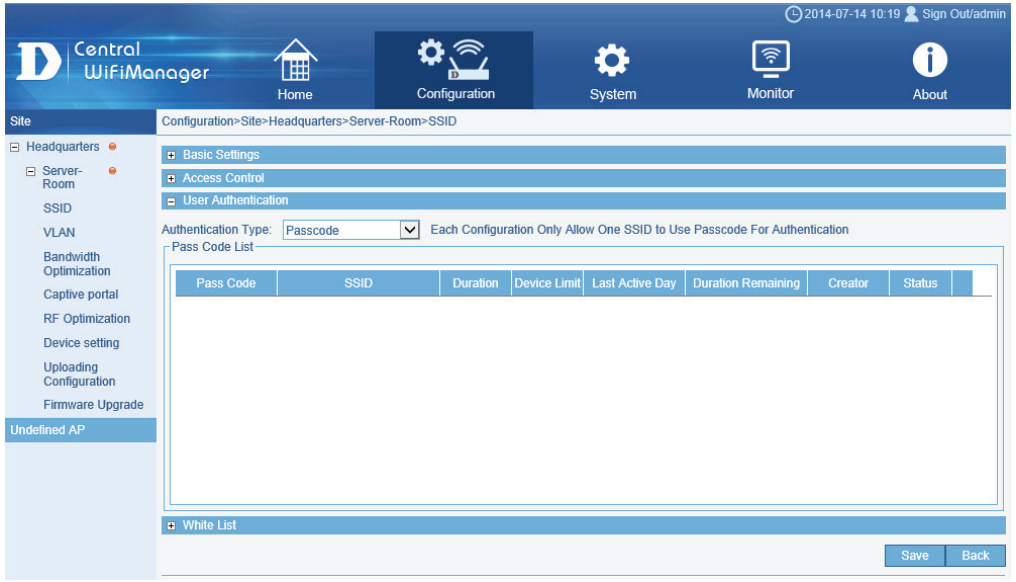
In this example, the guest network's SSID is called **SR-Guest**. To enable pass code user authentication for this SSID, click the button in the **SR-Guest** entry to modify the SSID.



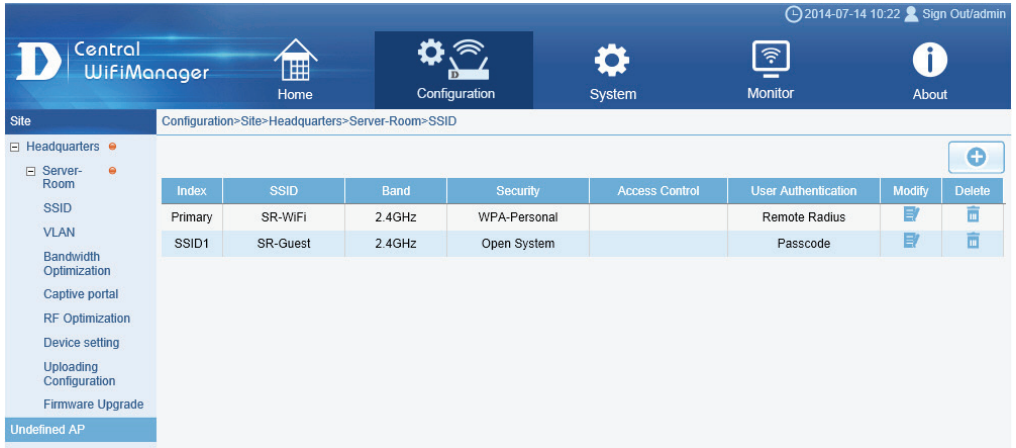
Appendix A - Front Desk Staff & User Access

After clicking the button, the following page will be available. Here we can modify the parameters of the SSID called **SR-Guest**.

In the **User Authentication** section, select **Passcode** as the **Authentication Type** and click the **Save** button to accept the changes made.



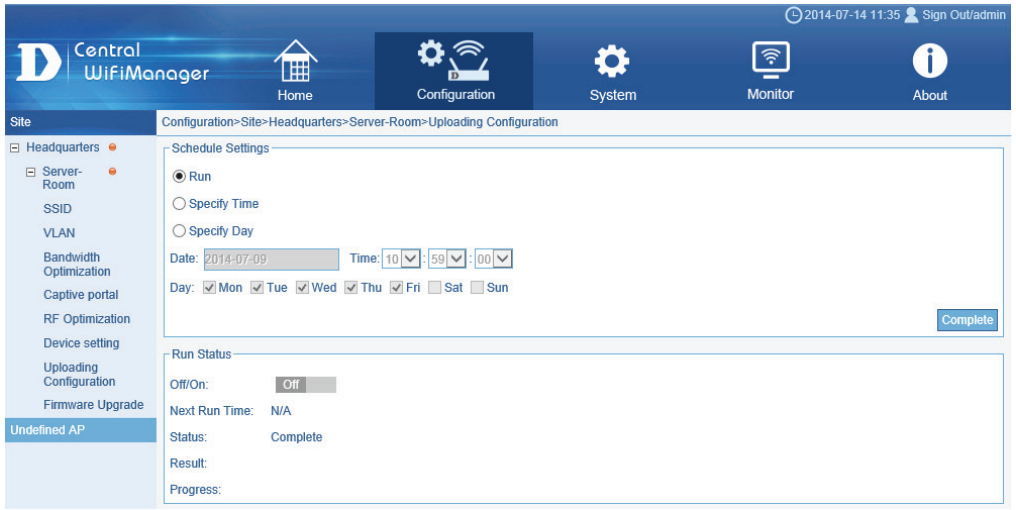
After successfully modifying the SSID to use pass codes for user authentication, the **User Authentication** entry column should display **Passcode** for the **SR-Guest** entry.



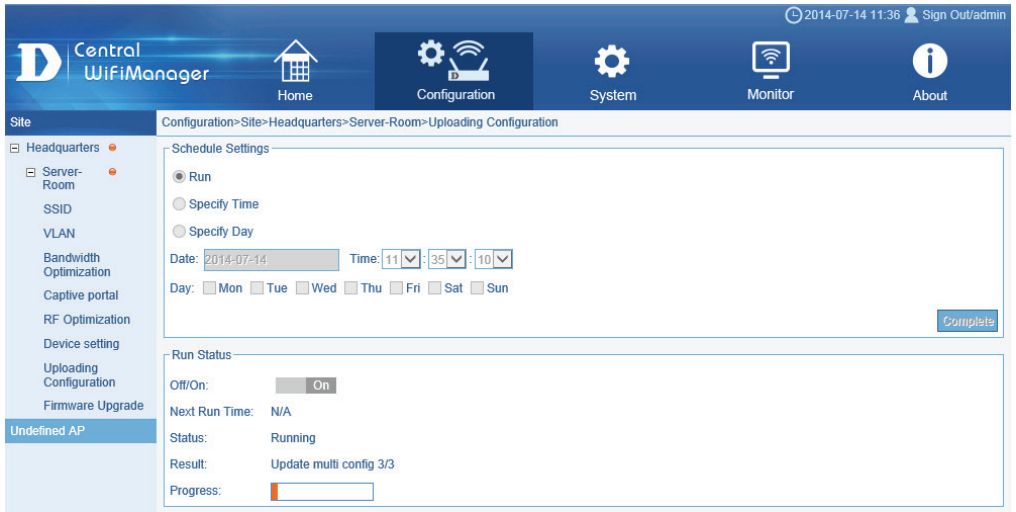
Appendix A - Front Desk Staff & User Access

Access points in the network, will not know about these new changes until the configuration of the relevant access points have been updated. To manually update the configuration of the relevant access points, navigate to **Configuration**, in the top menu, and your network link in the left menu. The network in this example is **Server-Room**.

Select the **Upload Configuration** option in the left menu. In the **Schedule Settings** section, select the **Run** option and click the **Complete** button.

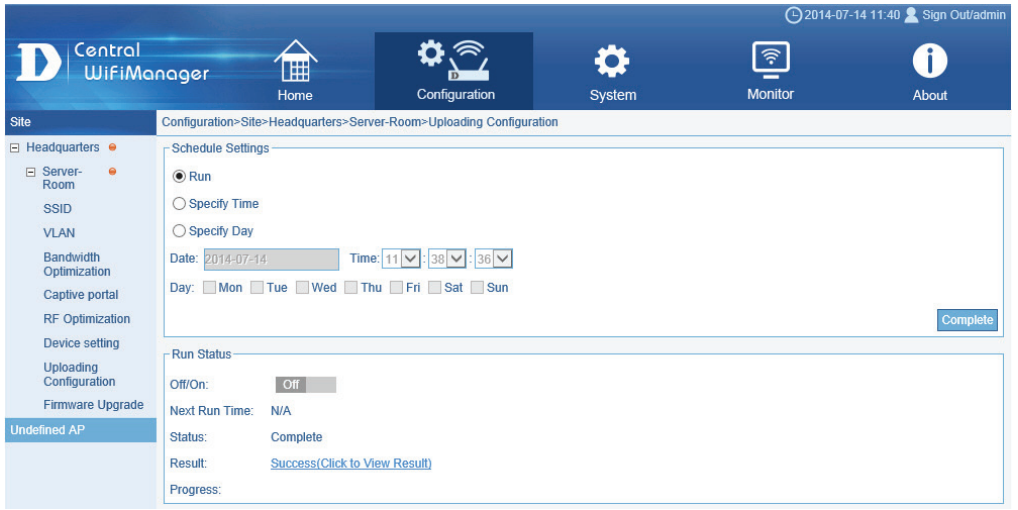


The configuration will now be uploaded to the relevant access points as displayed in the **Run Status** section.



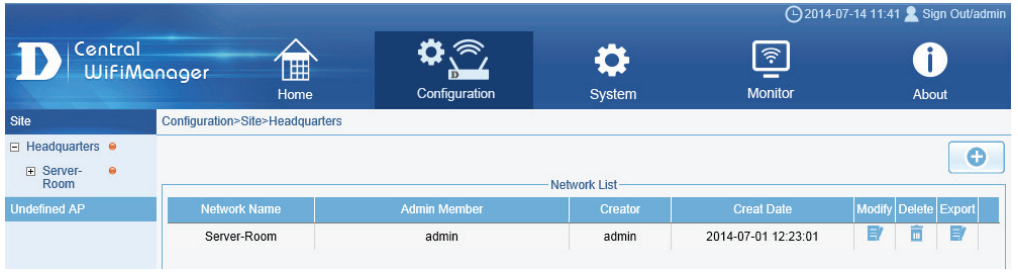
Appendix A - Front Desk Staff & User Access

After the configuration file was uploaded to the access points, the **Status** option in the **Run Status** section should show **Complete**.



Next we need to add the new front desk staff user account to the site's network member list. Navigate to the Configuration, in the top menu, and select the relevant site in the left menu. In this example our site's name is **Headquarters**.

All networks will be displayed in the **Network List** table. In this example, our network is called **Server-Room**. Click the button next to the entry, to modify this network.

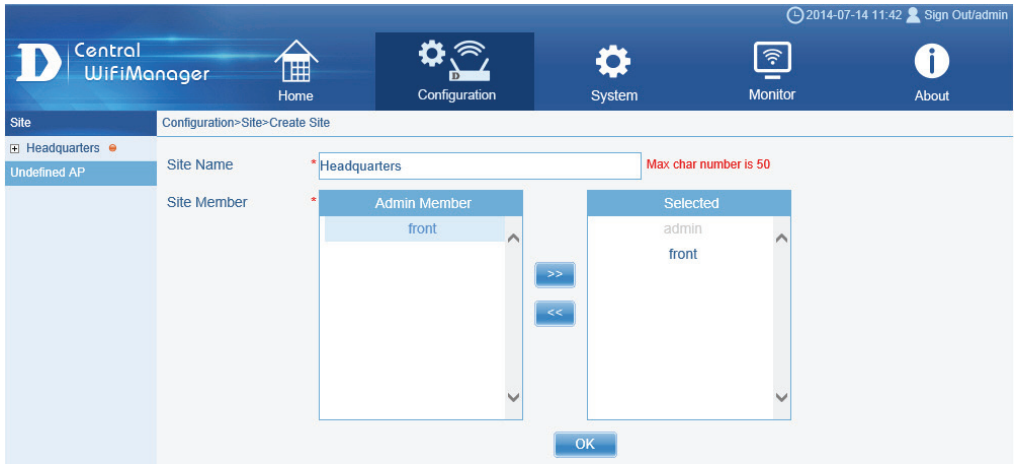


Appendix A - Front Desk Staff & User Access

After clicking the button, the following page will be available. The front desk staff user account will now be available and can be add to this network by selecting it and clicking on the **>>** button to move the account over to the **Selected** column.

Click the OK button to accept the changes made.

Click the **OK** button to accept the changes made.

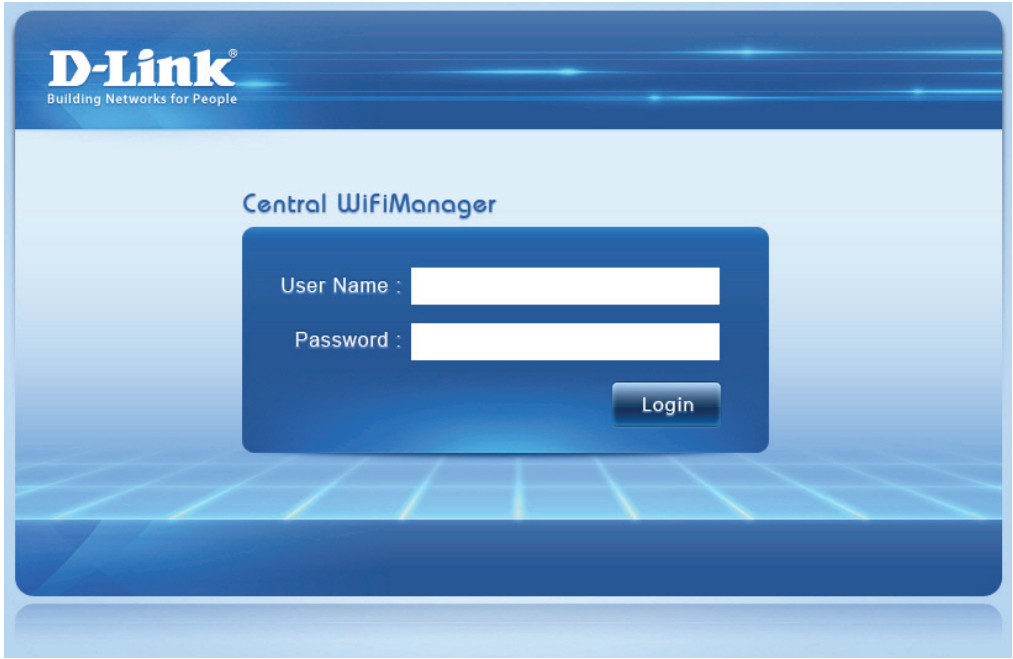


After this, upload the configuration files to the access points in the network again. Refer to the steps discussed earlier on how to do this.

Appendix A - Front Desk Staff & User Access

Now we can log out of the administrative account, and log back in with our front desk staff account.

Enter the front desk staff account's username and password in the spaces provided and click the **Login** button to enter the front desk staff account.

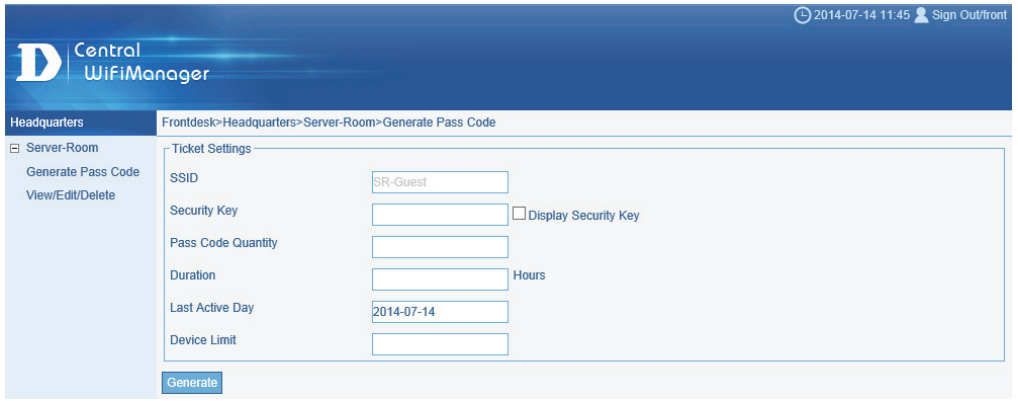


Appendix A - Front Desk Staff & User Access

After successfully logged in, using the front desk staff account, the following page will be available. On this page we can generate a pass code for front desk users.

The following parameters can be configured:

Parameter	Description
SSID	The network SSID will be displayed that front desk user can use to temporarily access the wireless network using the pass code that will be generated here.
Security Key	A pass code can be manually entered here. Leave this field blank to allow the system to generate a random pass code. Select the **Display Security Key** option to display the letter typed into this field.
Pass Code Quantity	Enter the amount of pass codes that will be generated here. Normally we'll only generate one pass code.
Duration	Enter the duration for this wireless connection here. This value must be in hours.
Last Active Day	Select the last active date that this code can be used here.
Device Limit	Enter the device limit value here. This is the maximum amount of active users that can use this pass code.



Click the **Generate** button to generate the new pass code.

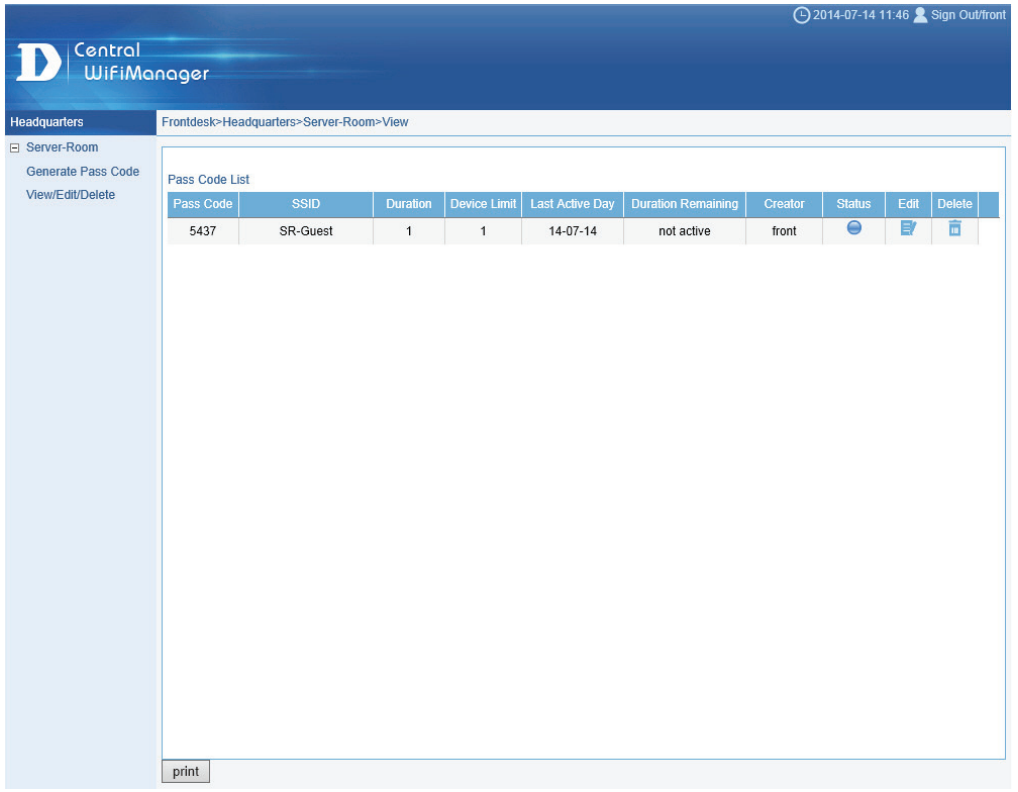
Appendix A - Front Desk Staff & User Access

After clicking on the **View/Edit/Delete** option in the left menu, we can view the list of pass codes that was generated. Also the **Duration Remaining** and **Status** fields are displayed here, that are useful for front desk staff to monitor active and passive connections.

Click the icon to modify an existing entry.
Click the icon to delete an existing entry.

Pass codes can now be given to front desk users by front desk staff.

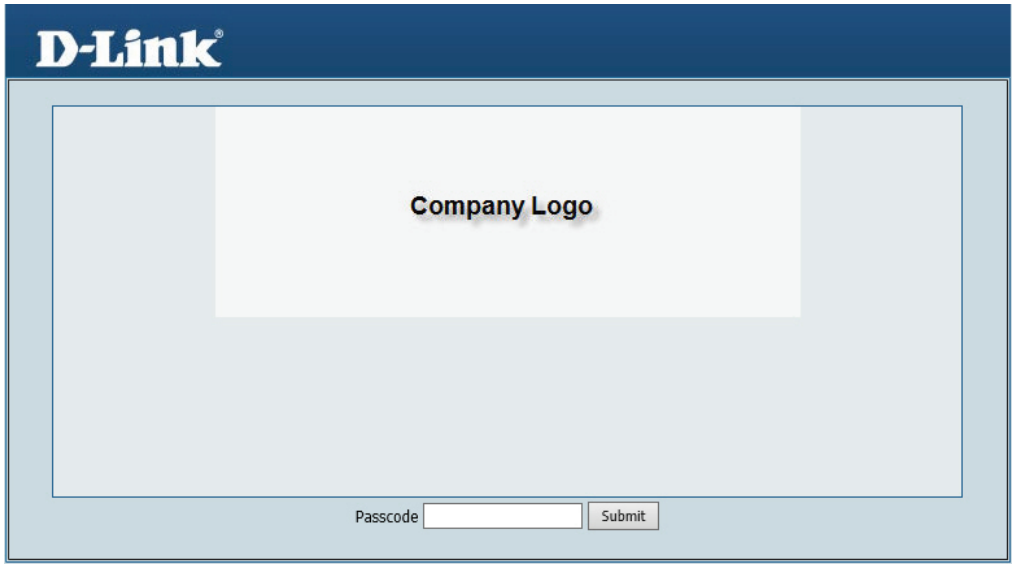
To generate new codes, front desk staff simply login to the Central WifiManager Server application, using the front desk staff user account details, enter the relevant ticket (pass code) information and click on the **Generate** button to get a code and give the code to the front desk user. Based on the **Duration** time specified, the ticket will expire and the entry can be removed.



Appendix A - Front Desk Staff & User Access

Front desk users simply connect to the wireless network available and when trying to connect to the network or Internet, using their Web browser, users will be asked to enter the pass code.

After entering the correct code, supplied by front desk staff, front desk users can connect to the network or Internet for the duration of the ticket.



Appendix B - Standard & Private Trap List

The Central WifiManager Server application uses a specific list of SNMP standard and private traps. Standard trap entries can be used in this application globally, however every access point, that was added into this application supports a very specific list of private trap entries that can only be configured and used for the specific access point's model name. In this appendix we'll list out all the standard and private trap list entries that can be viewed and configured in this application.

In the following table a list of **Standard** trap entries are displayed, that can be used in this application.

Event Name	SNMP Version	Generic Trap	Description	Level
ColdStart	SNMPv1	ColdStart(0)	The sending protocol entity has reinitialized,indicating that the agent's configuration nor entity implementation may be altered.	Notice
WarmStart	SNMPv1	WarmStart(1)	The sending protocol has reinitializing,but neither the agent's configuration or the protocol entity implementation has been altered.	Notice

In the following table a list of **Private** trap entries are displayed, that can be used in this application.

Event Name	SNMP Version	OID	Description	Level
DAP-2330deAuthentication	SNMPv1	1.3.6.1.4.1.171.10.37.5 1.5.7.2.20	Description needed	Critical
DAP-2330stationDisassocNotify	SNMPv1	1.3.6.1.4.1.171.10.37.5 1.5.7.2.15	Description needed	Critical

Appendix B - Standard & Private Trap List